Content delivery system and content delivery method

Patent Number: US2002099663
Publication date: 2002-07-25
Inventor(s): ISHIBASHI YOSHIHITO (JP); AKISHITA TORU (JP); YOSHINO KENJI (JP); OKA MAKOTO (JP); SHIRAI TAIZO (JP); YOSHIMORI MASAHARU (JP)
Applicant(s):
Requested Patent: JP2002141895
Application Number: US20010999456 20011031
Priority Number (s): JP20000334183 20001101
IPC Classification: G06F17/60
EC Classification: G06F17/60B
Equivalents: AU1520902, EP1237321, TW546937, WO0237746

Abstract

In a content delivery system, delivery of a content and charging for the fee of the content are performed and managed in a highly secure and effective fashion. If a content-purchasing request is transmitted from a user device to a shop server, a charging process is performed. If the charging process is successfully completed, the shop server transmits, to the user device, an encrypted content key in a form which can be decrypted by a key stored in the user device. A user device authentication server, which manages content delivery, converts an encrypted content key KpDAS(Kc) encrypted using a public key of the user device authentication server (DAS) into an encrypted content key KpDEV(Kc) encrypted using a public key KpDEV of the user device. Provided that the charging process has been successfully completed in response to the content-purchasing request, the shop server transmits the key-converted content key to the user device.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－141895
（P2002－141895A）
(43)公開日　平成14年５月17日(2002.5.17)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｈ０４Ｌ	9/08		Ｇ０６Ｆ	15/00	３３０Ｚ　５Ｂ０８５
Ｇ０６Ｆ	15/00	３３０		17/60	ＺＥＣ　５Ｃ０６４
	17/60	ＺＥＣ			１４２　５Ｊ１０４
		１４２			３０２Ｅ
		３０２			５１２

審査請求　未請求　請求項の数18　ＯＬ　（全 86 頁）　最終頁に続く

(21)出願番号　特願2000－334183(P2000－334183)

(22)出願日　平成12年11月１日(2000.11.1)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(71)出願人　395015319
株式会社ソニー・コンピュータエンタテインメント
東京都港区赤坂７－１－１

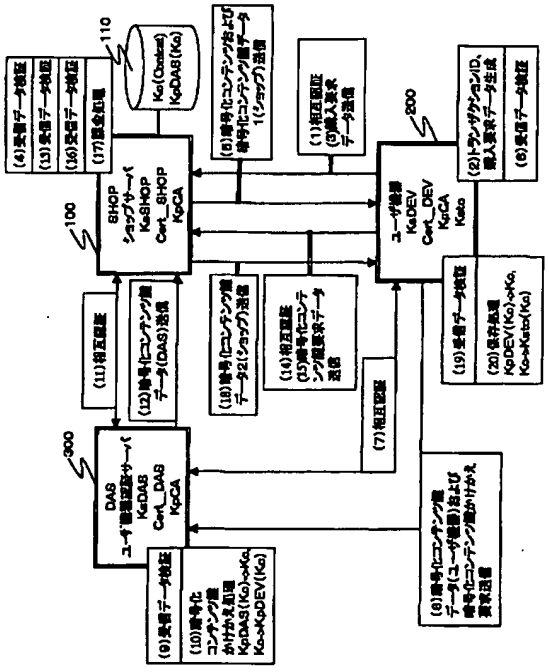
(72)発明者　吉野　賢治
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　コンテンツ配信システムおよびコンテンツ配信方法

(57)【要約】
【課題】　配信コンテンツの課金処理等の管理を確実にかつ効率的に行なうコンテンツ配信システムを提供する。
【解決手段】　ショップサーバが、ユーザ機器のコンテンツ購入要求に対する課金処理が終了したことを条件として、ユーザ機器の格納鍵での復号可能な態様とした暗号化コンテンツ鍵をユーザ機器に送付する。コンテンツ配信を管理するユーザ機器認証サーバが、ユーザ機器認証サーバ（ＤＡＳ）の公開鍵で暗号化したコンテンツ鍵ＫｐＤＡＳ（Ｋｃ）をユーザ機器の公開鍵ＫｐＤＥＶで暗号化したコンテンツ鍵ＫｐＤＥＶ（Ｋｃ）にかけかえる処理を実行する。コンテンツ購入要求に対する課金処理が終了したことを条件として、ショップサーバが鍵かけかえ済みのコンテンツ鍵をユーザ機器に送付する。



【特許請求の範囲】

【請求項１】ショップサーバに対してコンテンツ購入要求を送信するユーザ機器（ＤＥＶ）と、
前記ユーザ機器からのコンテンツ購入要求を受信するとともに、コンテンツ鍵Ｋｃで暗号化した暗号化コンテンツと、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵とを管理するショップサーバ（ＳＨＯＰ）と、
前記暗号化コンテンツ鍵を前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵とする鍵かけかえ処理を実行するユーザ機器認証サーバ（ＤＡＳ）とを有し、
前記ユーザ機器によるコンテンツ購入に基づく課金処理が完了したことを条件として、前記ユーザ機器認証サーバの生成したユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバから前記ユーザ機器に提供する構成としたことを特徴とするコンテンツ配信システム。

【請求項２】前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵は、前記ユーザ機器認証サーバ（ＤＡＳ）の公開鍵ＫｐＤＡＳで暗号化された暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）であり、
前記ユーザ機器認証サーバ（ＤＡＳ）の実行する鍵かけかえ処理は、前記暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を前記ユーザ機器認証サーバ（ＤＡＳ）の秘密鍵ＫｓＤＡＳで復号しコンテンツ鍵Ｋｃを取得し、さらに前記ユーザ機器（ＤＥＶ）の公開鍵ＫｐＤＥＶで再暗号化して暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）を生成する処理であることを特徴とする請求項１に記載のコンテンツ配信システム。

【請求項３】前記ユーザ機器認証サーバは、前記ユーザ機器から、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信し、
前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする請求項１に記載のコンテンツ配信システム。

【請求項４】前記ユーザ機器認証サーバは、前記ショップサーバから、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信し、
前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする請求項１に記載のコンテンツ配信システム。

【請求項５】前記コンテンツ配信システムは、さらに、前記ユーザ機器に対して暗号化コンテンツを配信する配信サーバを有し、
前記ショップサーバは、
前記ユーザ機器からのコンテンツ購入要求を受信に応じて、前記配信サーバに対してコンテンツ配信要求を送信する構成を有し、
前記配信サーバは、前記ショップサーバからのコンテンツ配信要求に応じて前記ユーザ機器に対して暗号化コンテンツを配信する処理を実行する構成を有することを特徴とする請求項１に記載のコンテンツ配信システム。

【請求項６】前記ユーザ機器が生成し、前記ショップサーバに対して送信するコンテンツ購入要求データは、
要求データ送信先であるショップの識別子としてのショップＩＤ、コンテンツ取り引き識別子としてのトランザクションＩＤ、購入要求対象のコンテンツ識別子としてのコンテンツＩＤを有するとともにユーザ機器の電子署名を含むデータとして構成され、
前記ショップサーバは、前記コンテンツ購入要求データの署名検証を実行することによりデータ改竄有無をチェックするとともに、該コンテンツ購入要求データに基づいて、ショップ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ショップでの処理シーケンス遷移を前記ステータス情報に基づいて管理する構成を有することを特徴とする請求項１に記載のコンテンツ配信システム。

【請求項７】前記ユーザ機器認証サーバは、前記ユーザ機器または前記ショップサーバのいずれかからの鍵かけかえ要求の受信に応じて、ユーザ機器認証サーバ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ユーザ機器認証サーバでの処理シーケンス遷移を前記ステータス情報に基づいて管理する構成を有することを特徴とする請求項１に記載のコンテンツ配信システム。

【請求項８】ショップサーバと、ユーザ機器間で取り引きされるコンテンツの配信管理を実行するユーザ機器認証サーバであり、
前記ショップサーバまたは前記ユーザ機器から受領する鍵かけかえ要求の受領に応じて、ショップサーバとユーザ機器間で取り引きされるコンテンツの暗号化鍵であるコンテンツ鍵を、前記ユーザ機器の格納鍵では復号不可能な態様で暗号化した暗号化コンテンツ鍵から前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵に変換する鍵かけかえ処理を実行する構成を有し、
前記ユーザ機器認証サーバは、前記鍵かけかえ要求中に含まれる前記ショップサーバの電子署名および、前記ユーザ機器の電子署名の検証を行ない、該検証により前記鍵かけかえ要求の正当性が確認されたことを条件として前記鍵かけかえ処理を実行する構成を有することを特徴とするユーザ機器認証サーバ。

【請求項９】ユーザ機器に対して暗号化コンテンツの復号に適用するコンテンツ鍵を提供するショップサーバであり、
コンテンツの暗号化鍵であるコンテンツ鍵を、前記ユーザ機器の格納鍵では復号不可能な態様で暗号化した暗号化コンテンツ鍵を管理し、
前記ユーザ機器からのコンテンツ購入要求に基づく課金処理の完了を条件として、コンテンツ配信を管理するユーザ機器認証サーバ（ＤＡＳ）が前記ユーザ機器の格納鍵では復号不可能な態様で暗号化した暗号化コンテンツ鍵の鍵かけかえ処理により生成する前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とするショップサーバ。
【請求項１０】前記ショップサーバは、暗号化コンテンツの配信サーバを含む構成であることを特徴とする請求項９に記載のショップサーバ。
【請求項１１】コンテンツの購入要求を生成しショップサーバに対して送信しコンテンツの再生処理を実行するコンテンツ再生機器であり、
コンテンツの配信管理を行なうユーザ機器認証サーバ（ＤＡＳ）の実行する鍵かけかえ処理により生成される前記コンテンツ再生機器の格納鍵により復号可能な暗号化コンテンツ鍵データをショップサーバを介して受信し、該受信する暗号化コンテンツ鍵データに含まれるショップサーバおよびユーザ機器認証サーバ（ＤＡＳ）の署名検証を実行し、データ改竄の無いことが確認されたことを条件として、受信した暗号化コンテンツ鍵データから暗号化コンテンツ鍵を取り出し復号しコンテンツ鍵の取得処理を実行する構成を有することを特徴とするコンテンツ再生機器。
【請求項１２】ユーザ機器（ＤＥＶ）からショップサーバ（ＳＨＯＰ）に対してコンテンツ購入要求を送信するステップと、
ショップサーバ（ＳＨＯＰ）において、前記ユーザ機器からのコンテンツ購入要求を受信するステップと、
ユーザ機器認証サーバ（ＤＡＳ）において、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵から、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵へ変換する鍵かけかえ処理を実行するステップと、
前記ショップサーバにおいて前記ユーザ機器によるコンテンツ購入に基づく課金処理が完了したことを条件として、前記ユーザ機器認証サーバの生成したユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバから前記ユーザ機器に提供するステップと、
を有することを特徴とするコンテンツ配信方法。
【請求項１３】前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵は、前記ユーザ機器認証サーバ（ＤＡＳ）の公開鍵ＫｐＤＡＳで暗号化された暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）であり、
前記ユーザ機器認証サーバ（ＤＡＳ）の実行する鍵かけかえ処理は、前記暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を前記ユーザ機器認証サーバ（ＤＡＳ）の秘密鍵ＫｓＤＡＳで復号しコンテンツ鍵Ｋｃを取得し、さらに前記ユーザ機器（ＤＥＶ）の公開鍵ＫｐＤＥＶで再暗号化して暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）を生成する処理であることを特徴とする請求項１２に記載のコンテンツ配信方法。
【請求項１４】前記ユーザ機器認証サーバは、前記ユーザ機器から、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信し、
前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする請求項１２に記載のコンテンツ配信方法。
【請求項１５】前記ユーザ機器認証サーバは、前記ショップサーバから、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信し、
前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする請求項１２に記載のコンテンツ配信方法。
【請求項１６】前記ユーザ機器が生成し、前記ショップサーバに対して送信するコンテンツ購入要求データは、要求データ送信先であるショップの識別子としてのショップＩＤ、コンテンツ取り引き識別子としてのトランザクションＩＤ、購入要求対象のコンテンツ識別子としてのコンテンツＩＤを有するとともにユーザ機器の電子署名を含むデータとして構成され、
前記ショップサーバは、前記コンテンツ購入要求データの署名検証を実行することによりデータ改竄有無をチェックするとともに、該コンテンツ購入要求データに基づいて、ショップ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ショップでの処理シーケンス遷移を前記ステータス情報に基づいて管理することを特徴とする請求項１２に記載のコンテンツ配信方法。
【請求項１７】前記ユーザ機器認証サーバは、前記ユーザ機器または前記ショップサーバのいずれかからの鍵かけかえ要求の受信に応じて、ユーザ機器認証サーバ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ユーザ機器認証サーバでの処理シーケンス遷移を前記ステ

ータス情報に基づいて管理することを特徴とする請求項１２に記載のコンテンツ配信方法。

【請求項１８】コンテンツ鍵の配信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

コンテンツ配信を管理するユーザ機器認証サーバ（ＤＡＳ）の生成するユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を受信するステップと、

前記ユーザ機器からのコンテンツ購入要求に基づく課金処理を実行するステップと、

前記課金処理の完了を条件として、前記ユーザ機器に対して、ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を送信するステップと、

を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はコンテンツ配信システムおよびコンテンツ配信方法に関する。さらに、詳細には、コンテンツ提供サービスを行なうエンティティと、コンテンツ受信を行なうユーザ機器間におけるコンテンツ取り引きにおけるセキュリティ、管理構成を改善したコンテンツ配信システムおよびコンテンツ配信方法に関する。なお、システムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【０００２】

【従来の技術】昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）の、インターネット等、ネットワークを介した流通が盛んになってきている。また、オンラインショッピング、銀行決済、チケット販売等のネットワークを介した商品売買、決済処理等も盛んになってきている。

【０００３】このようなネットワークを介したデータ通信においては、データ送信側とデータ受信側とが互いに正規なデータ送受信対象であることを確認した上で、必要な情報を転送する、すなわちセキュリティを考慮したデータ転送構成をとるのが一般的となっている。データ転送の際のセキュリティ構成を実現する手法には、転送データの暗号化処理、データに対する署名処理等がある。

【０００４】暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【０００５】暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その１つの例としていわゆる公開鍵暗号方式と呼ばれる方式がある。公開鍵暗号方式は、発信者と受信者の鍵を異なるものとして、一方の鍵を不特定のユーザが使用可能な公開鍵として、他方を秘密に保つ秘密鍵とするものである。例えば、データ暗号化鍵を公開鍵とし、復号鍵を秘密鍵とする。あるいは、認証子生成鍵を秘密鍵とし、認証子検証鍵を公開鍵とする等の態様において使用される。

【０００６】暗号化、復号化に共通の鍵を用いるいわゆる共通鍵暗号化方式と異なり、公開鍵暗号方式では秘密に保つ必要のある秘密鍵は、特定の１人が持てばよいため鍵の管理において有利である。ただし、公開鍵暗号方式は共通鍵暗号化方式に比較してデータ処理速度が遅く、秘密鍵の配送、ディジタル署名等のデータ量の少ない対象に多く用いられている。公開鍵暗号方式の代表的なものにはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。これは非常に大きな２つの素数（例えば１５０桁）の積を用いるものであり、大きな２つの素数（例えば１５０桁）の積の素因数分解する処理の困難さを利用している。

【０００７】公開鍵暗号方式では、不特定多数に公開鍵を使用可能とする構成であり、配布する公開鍵が正当なものであるか否かを証明する証明書、いわゆる公開鍵証明書を使用する方法が多く用いられている。例えば、利用者Ａが公開鍵、秘密鍵のペアを生成して、生成した公開鍵を認証局に対して送付して公開鍵証明書を認証局から入手する。利用者Ａは公開鍵証明書を一般に公開する。不特定のユーザは公開鍵証明書から所定の手続きを経て公開鍵を入手して文書等を暗号化して利用者Ａに送付する。利用者Ａは秘密鍵を用いて暗号化文書等を復号する等のシステムである。また、利用者Ａは、秘密鍵を用いて文書等に署名を付け、不特定のユーザが公開鍵証明書から所定の手続きを経て公開鍵を入手して、その署名の検証を行なうシステムである。

【０００８】公開鍵証明書は、公開鍵暗号方式における認証局あるいは発行局（ＣＡ：Certificate Authority またはＩＡ：Issuer Authority）が発行する証明書であり、ユーザが自己のＩＤ、公開鍵等を認証局に提出することにより、認証局側が認証局のＩＤや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【０００９】公開鍵証明書は、証明書のバージョン番号、発行局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前（ユーザＩＤ）、証明書利用者の公開鍵並びに電子署名を含む。

【００１０】電子署名は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵全体に対しハッシュ関数を

適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。

【００１１】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。

【００１２】

【発明が解決しようとする課題】上述のような認証局発行の公開鍵証明書を用いた公開鍵暗号方式によるデータ送信システムにおいては、例えばコンテンツを配信するコンテンツ配信ショップは、ユーザの公開鍵に基づいて配信対象のコンテンツを暗号化してユーザに送信する。コンテンツ配信ショップからの暗号化データを受信したユーザ機器は、自己の公開鍵に対応する自己の秘密鍵で暗号化コンテンツの復号を実行する。

【００１３】しかし、現実のコンテンツ取り引きにおいては、コンテンツの頒布権を持つライセンスホルダ、あるいはコンテンツの著作権を持つコンテンツ製作者は、コンテンツのユーザに対する提供サービスを行なうコンテンツ配信ショップとは異なる存在である場合が多く、コンテンツを受信しているユーザが、正当なコンテンツ利用権を有しているか否かについては、コンテンツ配信ショップは確認することなくコンテンツの配信を行なっていることが多い。すなわち、正当な利用権を持たないユーザによってコンテンツが不当に利用、あるいは販売される場合がある。

【００１４】また、上記のような取り引き形態においては、コンテンツの販売者であるコンテンツ配信ショップと、コンテンツ利用者であるユーザ機器の２者間においては相応のコンテンツ利用料を伴う取り引きが成立するが、コンテンツの頒布権を持つライセンスホルダ、あるいはコンテンツの著作権を持つコンテンツ製作者は、ショップとユーザ間のコンテンツ取り引きに伴うライセンス料の取得が保証されない。現状では、コンテンツ配信ショップの自己申告により、コンテンツの販売量を確認し、自己申告に基づくライセンス料が、ショップからライセンスホルダ、あるいはコンテンツ製作者等に提供されるのが一般的な取り引き形態である。

【００１５】このようなコンテンツ取り引き形態では、コンテンツの頒布権を持つライセンスホルダ、あるいはコンテンツの著作権を持つコンテンツ製作者は、コンテンツ取り引きの実体を把握できず、正確な利用権のもとで正当にコンテンツが流通しているか否かを確認する手段がなかった。

【００１６】本発明は、上述のような、コンテンツ取り引きにおける問題点に鑑みてなされたものであり、コンテンツの配信サービスを行なうコンテンツ配信ショップとユーザ間でのコンテンツ取り引きの実体をコンテンツの頒布権を持つライセンスホルダ、あるいはコンテンツの著作権を持つコンテンツ製作者において確実に把握可能とし、正当なコンテンツ利用権の管理のもとでコンテンツ配信を行なう構成としたコンテンツ配信システムおよびコンテンツ配信方法を提供するものである。

【００１７】

【課題を解決するための手段】本発明の第１の側面は、ショップサーバに対してコンテンツ購入要求を送信するユーザ機器（ＤＥＶ）と、前記ユーザ機器からのコンテンツ購入要求を受信するとともに、コンテンツ鍵Ｋｃで暗号化した暗号化コンテンツと、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵とを管理するショップサーバ（ＳＨＯＰ）と、前記暗号化コンテンツ鍵を前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵とする鍵かけかえ処理を実行するユーザ機器認証サーバ（ＤＡＳ）とを有し、前記ユーザ機器によるコンテンツ購入に基づく課金処理が完了したことを条件として、前記ユーザ機器認証サーバの生成したユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバから前記ユーザ機器に提供する構成としたことを特徴とするコンテンツ配信システムにある。

【００１８】さらに、本発明のコンテンツ配信システムの一実施態様において、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵は、前記ユーザ機器認証サーバ（ＤＡＳ）の公開鍵ＫｐＤＡＳで暗号化された暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）であり、前記ユーザ機器認証サーバ（ＤＡＳ）の実行する鍵かけかえ処理は、前記暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を前記ユーザ機器認証サーバ（ＤＡＳ）の秘密鍵ＫｓＤＡＳで復号しコンテンツ鍵Ｋｃを取得し、さらに前記ユーザ機器（ＤＥＶ）の公開鍵ＫｐＤＥＶで再暗号化して暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）を生成する処理であることを特徴とする。

【００１９】さらに、本発明のコンテンツ配信システムの一実施態様において、前記ユーザ機器認証サーバは、前記ユーザ機器から、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信し、前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする。

【００２０】さらに、本発明のコンテンツ配信システムの一実施態様において、前記ユーザ機器認証サーバは、前記ショップサーバから、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信

し、前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする。

【００２１】さらに、本発明のコンテンツ配信システムの一実施態様において、前記コンテンツ配信システムは、さらに、前記ユーザ機器に対して暗号化コンテンツを配信する配信サーバを有し、前記ショップサーバは、前記ユーザ機器からのコンテンツ購入要求を受信に応じて、前記配信サーバに対してコンテンツ配信要求を送信する構成を有し、前記配信サーバは、前記ショップサーバからのコンテンツ配信要求に応じて前記ユーザ機器に対して暗号化コンテンツを配信する処理を実行する構成を有することを特徴とする。

【００２２】さらに、本発明のコンテンツ配信システムの一実施態様において、前記ユーザ機器が生成し、前記ショップサーバに対して送信するコンテンツ購入要求データは、要求データ送信先であるショップの識別子としてのショップＩＤ、コンテンツ取り引き識別子としてのトランザクションＩＤ、購入要求対象のコンテンツ識別子としてのコンテンツＩＤを有するとともにユーザ機器の電子署名を含むデータとして構成され、前記ショップサーバは、前記コンテンツ購入要求データの署名検証を実行することによりデータ改竄有無をチェックするとともに、該コンテンツ購入要求データに基づいて、ショップ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ショップでの処理シーケンス遷移を前記ステータス情報に基づいて管理する構成を有することを特徴とする。

【００２３】さらに、本発明のコンテンツ配信システムの一実施態様において、前記ユーザ機器認証サーバは、前記ユーザ機器または前記ショップサーバのいずれかからの鍵かけかえ要求の受信に応じて、ユーザ機器認証サーバ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ユーザ機器認証サーバでの処理シーケンス遷移を前記ステータス情報に基づいて管理する構成を有することを特徴とする。

【００２４】さらに、本発明の第２の側面は、ショップサーバと、ユーザ機器間で取り引きされるコンテンツの配信管理を実行するユーザ機器認証サーバであり、前記ショップサーバまたは前記ユーザ機器から受領する鍵かけかえ要求の受領に応じて、ショップサーバとユーザ機器間で取り引きされるコンテンツの暗号化鍵であるコンテンツ鍵を、前記ユーザ機器の格納鍵では復号不可能な態様で暗号化した暗号化コンテンツ鍵から前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵に変換する鍵かけかえ処理を実行する構成を有し、前記ユーザ機器認証サーバは、前記鍵かけかえ要求中に含まれる前記ショップサーバの電子署名および、前記ユーザ機器の電子署名の検証を行ない、該検証により前記鍵かけかえ要求の正当性が確認されたことを条件として前記鍵かけかえ処理を実行する構成を有することを特徴とするユーザ機器認証サーバにある。

【００２５】さらに、本発明の第３の側面は、ユーザ機器に対して暗号化コンテンツの復号に適用するコンテンツ鍵を提供するショップサーバであり、コンテンツの暗号化鍵であるコンテンツ鍵を、前記ユーザ機器の格納鍵では復号不可能な態様で暗号化した暗号化コンテンツ鍵を管理し、前記ユーザ機器からのコンテンツ購入要求に基づく課金処理の完了を条件として、コンテンツ配信を管理するユーザ機器認証サーバ（ＤＡＳ）が前記ユーザ機器の格納鍵では復号不可能な態様で暗号化した暗号化コンテンツ鍵の鍵かけかえ処理により生成する前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とするショップサーバにある。

【００２６】さらに、本発明のショップサーバの一実施態様において、前記ショップサーバは、暗号化コンテンツの配信サーバを含む構成であることを特徴とする。

【００２７】さらに、本発明の第４の側面は、コンテンツの購入要求を生成しショップサーバに対して送信しコンテンツの再生処理を実行するコンテンツ再生機器であり、コンテンツの配信管理を行なうユーザ機器認証サーバ（ＤＡＳ）の実行する鍵かけかえ処理により生成される前記コンテンツ再生機器の格納鍵により復号可能な暗号化コンテンツ鍵データをショップサーバを介して受信し、該受信する暗号化コンテンツ鍵データに含まれるショップサーバおよびユーザ機器認証サーバ（ＤＡＳ）の署名検証を実行し、データ改竄の無いことが確認されたことを条件として、受信した暗号化コンテンツ鍵データから暗号化コンテンツ鍵を取り出し復号しコンテンツ鍵の取得処理を実行する構成を有することを特徴とするコンテンツ再生機器にある。

【００２８】さらに、本発明の第５の側面は、ユーザ機器（ＤＥＶ）からショップサーバ（ＳＨＯＰ）に対してコンテンツ購入要求を送信するステップと、ショップサーバ（ＳＨＯＰ）において、前記ユーザ機器からのコンテンツ購入要求を受信するステップと、ユーザ機器認証サーバ（ＤＡＳ）において、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵から、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵へ変換する鍵かけかえ処理を実行するステップと、前記ショップサーバにおいて前記ユーザ機器によるコンテンツ購入に基づく課金処理が完了したことを条件として、前記ユーザ機器認証サーバの生成したユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバから前記ユーザ機器に提供するステップと、を有することを特徴とするコンテンツ配信方法にある。

【００２９】さらに、本発明のコンテンツ配信方法の一実施態様において、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵は、前記ユーザ機器認証サーバ（ＤＡＳ）の公開鍵ＫｐＤＡＳで暗号化された暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）であり、前記ユーザ機器認証サーバ（ＤＡＳ）の実行する鍵かけかえ処理は、前記暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を前記ユーザ機器認証サーバ（ＤＡＳ）の秘密鍵ＫｓＤＡＳで復号しコンテンツ鍵Ｋｃを取得し、さらに前記ユーザ機器（ＤＥＶ）の公開鍵ＫｐＤＥＶで再暗号化して暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）を生成する処理であることを特徴とする。

【００３０】さらに、本発明のコンテンツ配信方法の一実施態様において、前記ユーザ機器認証サーバは、前記ユーザ機器から、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信し、前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする。

【００３１】さらに、本発明のコンテンツ配信方法の一実施態様において、前記ユーザ機器認証サーバは、前記ショップサーバから、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信し、前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする。

【００３２】さらに、本発明のコンテンツ配信方法の一実施態様において、前記ユーザ機器が生成し、前記ショップサーバに対して送信するコンテンツ購入要求データは、要求データ送信先であるショップの識別子としてのショップＩＤ、コンテンツ取り引き識別子としてのトランザクションＩＤ、購入要求対象のコンテンツ識別子としてのコンテンツＩＤを有するとともにユーザ機器の電子署名を含むデータとして構成され、前記ショップサーバは、前記コンテンツ購入要求データの署名検証を実行することによりデータ改竄有無をチェックするとともに、該コンテンツ購入要求データに基づいて、ショップ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ショップでの処理シーケンス遷移を前記ステータス情報に基づいて管理することを特徴とする。

【００３３】さらに、本発明のコンテンツ配信方法の一実施態様において、前記ユーザ機器認証サーバは、前記ユーザ機器または前記ショップサーバのいずれかからの鍵かけかえ要求の受信に応じて、ユーザ機器認証サーバ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ユーザ機器認証サーバでの処理シーケンス遷移を前記ステータス情報に基づいて管理することを特徴とする。

【００３４】さらに、本発明の第６の側面は、コンテンツ鍵の配信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、コンテンツ配信を管理するユーザ機器認証サーバ（ＤＡＳ）の生成するユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を受信するステップと、前記ユーザ機器からのコンテンツ購入要求に基づく課金処理を実行するステップと、前記課金処理の完了を条件として、前記ユーザ機器に対して、ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を送信するステップと、を有することを特徴とするプログラム提供媒体にある。

【００３５】なお、本発明の第６の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００３６】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００３７】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００３８】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態について詳細に説明する。なお、説明は、以下の項目に従って行なう。

１．暗号化コンテンツ鍵の鍵かけかえ処理によるコンテンツ配信管理

１．１．システム構成：基本コンテンツ配信モデル１

１．２．基本コンテンツ配信モデル１の変形例

１．３．基本コンテンツ配信モデル２

２．電子チケットを利用したコンテンツ配信モデル

３．ログ収集サーバによるコンテンツ配信管理

４．属性データを記録した公開鍵証明書または属性証明書利用構成

【００３９】

【実施例】［1．暗号化コンテンツ鍵の鍵かけかえ処理によるコンテンツ配信管理］

［1．1．システム構成：基本コンテンツ配信モデル1］図1に本発明のコンテンツ配信システムおよびコンテンツ配信方法の一実施例の概要を説明する図を示す。なお、システムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【００４０】図1のコンテンツ配信システムは、ユーザ機器に対するコンテンツの配信サービスを行なうショップサーバ（ＳＨＯＰ）１００、ショップサーバ１００からのコンテンツ配信を受信するユーザ機器（ＤＥＶＩＣＥ）２００、さらに、正当なコンテンツ取り引き管理を行なう管理サーバとして機能するユーザ機器認証サーバ（ＤＡＳ：Device Authentication Server）３００を主構成要素とする。なお、図1の構成では、ショップサーバ１００、ユーザ機器２００、ユーザ機器認証サーバ３００を1つづつ示しているが、実際のコンテンツ取り引き構成においては、図1に示す各構成要素が複数存在し、各コンテンツ取り引き毎に、様々なルートで情報が送受信される。図1は、1つのコンテンツ取り引きにおけるデータの流れを示しているものである。

【００４１】（ショップサーバ）図1のコンテンツ配信システムのショップサーバ１００の構成を図2に示す。ショップサーバ１００は、取り引き対象となるコンテンツをコンテンツキーで暗号化した暗号化コンテンツデータであるＫｃ（Ｃｏｎｔｅｎｔ）と、コンテンツキーＫｃをユーザ機器認証サーバ（ＤＡＳ：Device Authentication Server）の公開鍵：ＫｐＤＡＳで暗号化した暗号化コンテンツキーＫｐＤＡＳ（Ｋｃ）を格納したコンテンツデータベース１１０を有する。なお、暗号化コンテンツデータであるＫｃ（Ｃｏｎｔｅｎｔ）は、図にも示すように、それぞれコンテンツ識別子であるコンテンツＩＤが付加され、コンテンツＩＤに基づいて識別可能な構成を持つ。

【００４２】ショップサーバ１００は、さらにコンテンツ取り引き管理データ、例えばコンテンツ販売先のユーザ機器の識別子とコンテンツ識別子等を対応づけて管理する購買管理データベース１２０を有する。さらに、コンテンツデータベース１１０からの配信コンテンツの抽出処理、取り引きに伴う購買管理データベース１２０に対して登録する取り引きデータの生成処理、ユーザ機器２００、ユーザ機器認証サーバ３００との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段１３０を有する。

【００４３】購買管理データベース１２０のデータ構成を図3に示す。購買管理データベース１２０は、ショップサーバがコンテンツ取り引きに応じて処理を実行する際に内部生成する識別番号としてのショップ処理Ｎｏ．、コンテンツ購入依頼を発行したユーザ機器の識別子である機器ＩＤ、ユーザ機器とショップ間でのコンテンツ取り引きを実行する際に、ユーザ機器で生成発行するコンテンツ取り引き識別子としてのトランザクションＩＤ、取り引き対象コンテンツの識別子であるコンテンツＩＤ、ショップサーバにおけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【００４４】制御手段１３０は、図2に示すように暗号処理手段、通信処理手段としての機能も有し、制御手段１３０は、例えば暗号処理プログラム、通信処理プログラムを格納したコンピュータによって構成される。制御手段１３０の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。ショップサーバ１００が格納する暗号鍵等の暗号処理用データとしては、ショップサーバの秘密鍵：ＫｓＳＨＯＰ、ショップサーバの公開鍵証明書Ｃｅｒｔ＿ＳＨＯＰ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡがある。

【００４５】図4に制御手段１３０の構成例を示す。制御手段１３０の構成について説明する。制御部１３１は各種処理プログラムを実行する中央演算処理装置（ＣＰＵ:Central Processing Unit）によって構成され、図4の制御手段の各構成部位の処理を制御する。ＲＯＭ（Read only Memory）１３２は、ＩＰＬ（Initial Program Loading）等のプログラムを記憶したメモリである。ＲＡＭ（Random Access Memory）１３３は、制御部１３１が実行するプログラム、例えばデータベース管理プログラム、暗号処理プログラム、通信プログラム等、実行プログラムの格納領域、またこれら各プログラム処理におけるワークエリアとして使用される。

【００４６】表示部１３４は、液晶表示装置、ＣＲＴなどの表示手段を有し、制御部１３１の制御の下、様々なプログラム実行時のデータ、例えばコンテンツ配信先のユーザデータ等を表示する。入力部１３５は、キーボードや、例えばマウス等のポインティングデバイスを有し、これら各入力デバイスからのコマンド、データ入力を制御部１３１に出力する。ＨＤＤ（Hard Disk Drive）１３６は、データベース管理プログラム、暗号処理プログラム、通信プログラム等のプログラム、さらに各種データが格納される。

【００４７】ドライブ１３７は、例えばＨＤ（Hard Disk）や、ＦＤ（Floppy Disk）等の磁気ディスク、ＣＤ－ＲＯＭ（Compact Disk ROM）などの光ディスク、ミニディスク等の光磁気ディスク、ＲＯＭやフラッシュメモリなどの半導体メモリ等の各種記録媒体に対するアクセスを制御する機能を持つ。磁気ディスク等の各種記録媒体はプログラム、データ等を記憶する。ネットワークイン

タフェース１３８は、インターネット、電話回線等の有線、無線を介した通信のインタフェースとして機能する。

【００４８】ショップサーバ１００は、例えば上述した構成を持つ制御手段１３０において、コンテンツの取り引き対象であるユーザ機器２００、あるいはユーザ機器認証サーバ３００との間でのコンテンツ取り引きに伴う様々な暗号処理、認証処理等を実行する。

【００４９】（ユーザ機器認証サーバ）図５にユーザ機器認証サーバ（ＤＡＳ）３００の構成を示す。ユーザ機器認証サーバは、ライセンス管理データベース３２０を有する。ライセンス管理データベース３２０のデータ構成を図６に示す。ライセンス管理データベースは、コンテンツ取り引き時にユーザ機器認証サーバ（ＤＡＳ）の実行する処理に応じて内部生成する処理識別子としてのユーザ機器認証サーバ処理Ｎｏ．、コンテンツ購入依頼を発行したユーザ機器の識別子である機器ＩＤ、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するコンテンツ取り引き識別子としてのトランザクションＩＤ、取り引き対象コンテンツの識別子であるコンテンツＩＤ、コンテンツ取り引きを実行するショップサーバの識別子であるショップＩＤ、ショップの発行するショップでの処理識別子であるショップ処理Ｎｏ．、ユーザ機器認証サーバ（ＤＡＳ）におけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される

【００５０】ユーザ機器認証サーバ（ＤＡＳ）３００は、ユーザ機器２００、ショップサーバ１００との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段３３０を有する。制御手段３３０は、先に説明したショップサーバの制御手段と同様、暗号処理手段、通信処理手段としての機能も有する。その構成は、図４を用いて説明した構成と同様である。制御手段３３０の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。ユーザ機器認証サーバ（ＤＡＳ）３００が格納する暗号鍵等の暗号処理用データとしては、ユーザ機器認証サーバ（ＤＡＳ）の秘密鍵：ＫｓＤＡＳ、ユーザ機器認証サーバ（ＤＡＳ）の公開鍵証明書Ｃｅｒｔ＿ＤＡＳ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡがある。

【００５１】（ユーザ機器）図７にユーザ機器２００の構成を示す。ユーザ機器は、コンテンツの購入を実行し、購入したコンテンツの利用、すなわちコンテンツ再生、実行を行なう例えばコンテンツ再生機器であり、購入管理データベース２２０を有する。購入管理データベース２２０のデータ構成を図８に示す。購入管理データベースは、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するコンテンツ取り引き識別子としてのトランザクションＩＤ、取り引き対象コンテンツの識別子であるコンテンツＩＤ、コンテンツ取り引きを実行するショップサーバの識別子であるショップＩＤ、ユーザ機器におけるコンテンツ取り引き処理のステータスを示すステータスの各情報、さらに、ユーザ機器の機器識別子である機器ＩＤを持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【００５２】ユーザ機器２００は、ショップサーバ１００、ユーザ機器認証サーバ３００との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段２３０を有する。制御手段２３０は、先に説明したショップサーバの制御手段と同様、暗号処理手段、通信処理手段としての機能も有する。その構成は、図４を用いて説明した構成と同様である。制御手段２３０の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。ユーザ機器２００が格納する暗号鍵等の暗号処理用データとしては、ユーザ機器の秘密鍵：ＫｓＤＥＶ、ユーザ機器の公開鍵証明書Ｃｅｒｔ＿ＤＥＶ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡ、コンテンツをユーザ機器の例えばハードディスク等の記憶手段に格納する際の暗号化鍵として適用する保存鍵Ｋｓｔｏがある。

【００５３】［公開鍵証明書］上記ショップサーバ（ＳＨＯＰ）１００、ユーザ機器（ＤＥＶＩＣＥ）２００、ユーザ機器認証サーバ（ＤＡＳ：Device Authentication Server）３００の保有する公開鍵証明書について図９を用いて説明する。

【００５４】公開鍵証明書は、公開鍵を用いた暗号データの送受信、あるいはデータ送受信を行なう２者間での相互認証等の処理において、使用する公開鍵が正当な利用者の有する公開鍵であることを第三者、すなわち発行局（ＣＡ：Certificate Authority）が証明したものである。公開鍵証明書のフォーマットの概略を図９（ａ）に示す。

【００５５】バージョン（version）は、証明書フォーマットのバージョンを示す。証明書の通し番号は、シリアルナンバ（Serial Number）であり、公開鍵証明書発行局（ＣＡ）によって設定される公開鍵証明書のシリアルナンバである。署名アルゴリズム識別子、アルゴリズムパラメータ（Signature algorithm Identifier algorithm parameter）は、公開鍵証明書の署名アルゴリズムとそのパラメータを記録するフィールドである。なお、署名アルゴリズムとしては、楕円曲線暗号およびＲＳＡがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、ＲＳＡが適用されている場合には鍵長が記録される。発行局の名前は、公開鍵証明書

の発行者、すなわち公開鍵証明書発行局（ＣＡ）の名称が識別可能な形式（Distinguished Name）で記録されるフィールドである。証明書の有効期限(validity)は、証明書の有効期限である開始日時、終了日時が記録される。公開鍵証明書の利用者名（ＩＤ）は、ユーザである認証対象者の名前が記録される。具体的には例えばユーザ機器のＩＤや、サービス提供主体のＩＤ等である。利用者公開鍵（subject Public Key Info algorithm subject Public key）は、ユーザの公開鍵情報としての鍵アルゴリズム、鍵情報そのものを格納するフィールドである。発行局が付ける署名は、公開鍵証明書発行局（ＣＡ）の秘密鍵を用いて公開鍵証明書のデータに対して実行される電子署名であり、公開鍵証明書の利用者は、公開鍵証明書発行局（ＣＡ）の公開鍵を用いて検証を行ない、公開鍵証明書の改竄有無がチェック可能となっている。

【００５６】公開鍵暗号方式を用いた電子署名の生成方法について、図１０を用いて説明する。図１０に示す処理は、ＥＣ－ＤＳＡ（（Elliptic Curve Digital SignatureAlgorithm）、IEEE P1363/D3）を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号（Elliptic Curve Cryptography（以下、ＥＣＣと呼ぶ））を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばＲＳＡ暗号（（Rivest、Shamir、Adleman）など（ANSI X9.31））を用いることも可能である。

【００５７】図１０の各ステップについて説明する。ステップＳ１において、ｐを標数、a、bを楕円曲線の係数（楕円曲線：$4a^3+27b^2\neq 0$（ｍｏｄ　ｐ）、Ｇを楕円曲線上のベースポイント、rをＧの位数、Ｋｓを秘密鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ２おいて、メッセージMのハッシュ値を計算し、f=Hash(M)とする。

【００５８】ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、ＭＤ４、ＭＤ５、ＳＨＡ－１などが用いられる場合もあるし、ＤＥＳ－ＣＢＣが用いられる場合もある。この場合は、最終出力値となるＭＡＣ（チェック値：ＩＣＶに相当する）がハッシュ値となる。

【００５９】続けて、ステップＳ３で、乱数ｕ（０＜ｕ＜ｒ）を生成し、ステップＳ４でベースポイントをｕ倍した座標Ｖ（Ｘｖ，Ｙｖ）を計算する。なお、楕円曲線上の加算、２倍算は次のように定義されている。

【００６０】

【数１】P=(Ｘａ，Ｙａ),Q=(Ｘｂ，Ｙｂ),R=(Ｘｃ,Ｙｃ)=P+Qとすると、P≠Qの時（加算）、

$Xc=\lambda^2-Xa-Xb$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(Yb-Ya)/(Xb-Xa)$

P=Qの時（2倍算）、

$Xc=\lambda^2-2Xa$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(3(Xa)^2+a)/(2Ya)$

【００６１】これらを用いて点Ｇのｕ倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。Ｇ、２×Ｇ、４×Ｇ・・を計算し、uを2進数展開して1が立っているところに対応する$2^i\times G$（Ｇをｉ回２倍算した値（ｉはｕのＬＳＢから数えた時のビット位置））を加算する。

【００６２】ステップＳ５で、ｃ＝Ｘｖｍｏｄ　ｒを計算し、ステップＳ６でこの値が０になるかどうか判定し、０でなければステップＳ７でｄ＝［（ｆ＋ｃＫｓ）／ｕ］ｍｏｄ　ｒを計算し、ステップＳ８でｄが０であるかどうか判定し、ｄが０でなければ、ステップＳ９でｃおよびｄを電子署名データとして出力する。仮に、ｒを１６０ビット長の長さであると仮定すると、電子署名データは３２０ビット長となる。

【００６３】ステップＳ６において、ｃが０であった場合、ステップＳ３に戻って新たな乱数を生成し直す。同様に、ステップＳ８でｄが０であった場合も、ステップＳ３に戻って乱数を生成し直す。

【００６４】次に、公開鍵暗号方式を用いた電子署名の検証方法を、図１１を用いて説明する。ステップＳ１１で、Ｍをメッセージ、ｐを標数、a、bを楕円曲線の係数（楕円曲線：$y^2=x^3+ax+b$）、Ｇを楕円曲線上のベースポイント、rをＧの位数、ＧおよびＫｓ×Ｇを公開鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ１２で電子署名データｃおよびｄが０＜ｃ＜ｒ、０＜ｄ＜ｒを満たすか検証する。これを満たしていた場合、ステップＳ１３で、メッセージMのハッシュ値を計算し、ｆ＝Ｈａｓｈ（Ｍ）とする。次に、ステップＳ１４でh=1/d mod rを計算し、ステップＳ１５でｈ１＝ｆｈ　ｍｏｄ　ｒ、ｈ２＝ｃｈ　ｍｏｄ　ｒを計算する。

【００６５】ステップＳ１６において、既に計算したｈ１およびｈ２を用い、点Ｐ＝（Ｘｐ，Ｙｐ）＝ｈ１×Ｇ＋ｈ２・Ｋｓ×Ｇを計算する。電子署名検証者は、公開鍵ＧおよびＫｓ×Ｇを知っているので、図１０のステップＳ４と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップＳ１７で点Ｐが無限遠点かどうか判定し、無限遠点でなければステップＳ１８に進む（実際には、無限遠点の判定はステップＳ１６でできてしまう。つまり、Ｐ＝（Ｘ，Ｙ）、Ｑ＝（Ｘ，－Ｙ）の加算を行うと、λが計算できず、Ｐ＋Ｑが無限遠点であ

ることが判明している）。ステップＳ１８でＸｐ ｍｏｄ ｒを計算し、電子署名データｃと比較する。最後に、この値が一致していた場合、ステップＳ１９に進み、電子署名が正しいと判定する。

【００６６】電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【００６７】ステップＳ１２において、電子署名データｃまたはｄが、０＜ｃ＜ｒ、０＜ｄ＜ｒを満たさなかった場合、ステップＳ２０に進む。また、ステップＳ１７において、点Ｐが無限遠点であった場合もステップＳ２０に進む。さらにまた、ステップＳ１８において、Ｘｐ ｍｏｄ ｒの値が、電子署名データｃと一致していなかった場合にもステップＳ２０に進む。

【００６８】ステップＳ２０において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。

【００６９】公開鍵証明書には、発行局の署名がなされ、公開鍵利用者による署名検証により、証明書の改竄がチェック可能な構成となっている。図９に戻り説明をつづける。図９（ｂ）がユーザ機器に格納されるユーザ機器の公開鍵証明書：Ｃｅｒｔ＿ＤＥＶであり、ユーザ機器ＩＤと、ユーザ機器の公開鍵ＫｐＤＥＶを格納している。図９（ｃ）はショップサーバに格納されるショップサーバの公開鍵証明書：Ｃｅｒｔ＿ＳＨＯＰであり、ショップＩＤと、ショップサーバの公開鍵ＫｐＳＨＯＰを格納している。図９（ｄ）はユーザ機器認証サーバに格納されるユーザ機器認証サーバの公開鍵証明書：Ｃｅｒｔ＿ＤＡＳであり、ユーザ機器認証サーバＩＤと、ユーザ機器認証サーバの公開鍵ＫｐＤＡＳを格納している。このように、ユーザ機器、ショップサーバ、ユーザ機器認証サーバがそれぞれ公開鍵証明書を保有する。

【００７０】［コンテンツ購入処理］次に、図１に戻り、ユーザ機器が、ショップサーバからコンテンツを購入して利用する処理について説明する。図１の番号（１）から（２０）の順に処理が進行する。各番号順に処理の詳細を説明する。なお、本実施例ではエンティティ間の通信において相互認証処理（（１）、（７）、（１１））を行なったものを述べているが、必要に応じて省略しても構わない。

【００７１】（１）相互認証

コンテンツをショップサーバ１００から購入しようとするユーザ機器２００は、ショップサーバとの間で相互認証処理を行なう。データ送受信を実行する２つの手段間では、相互に相手が正しいデータ通信者であるか否かを確認して、その後に必要なデータ転送を行なうことが行われる。相手が正しいデータ通信者であるか否かの確認処理が相互認証処理である。相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が１つの好ましいデータ転送方式である。

【００７２】共通鍵暗号方式を用いた相互認証方法を、図１２を用いて説明する。図１２において、共通鍵暗号方式としてＤＥＳを用いているが、同様な共通鍵暗号方式であればいずれでもよい。

【００７３】まず、Ｂが６４ビットの乱数Ｒｂを生成し、Ｒｂおよび自己のＩＤであるＩＤ（ｂ）をＡに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａを生成し、Ｒａ、Ｒｂ、ＩＤ（ｂ）の順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いてデータを暗号化し、Ｂに返送する。

【００７４】これを受信したＢは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、まず、暗号文Ｅ１を鍵Ｋａｂで復号化し、乱数Ｒａを得る。次に、暗号文Ｅ２を鍵Ｋａｂで復号化し、その結果とＥ１を排他的論理和し、Ｒｂを得る。最後に、暗号文Ｅ３を鍵Ｋａｂで復号化し、その結果とＥ２を排他的論理和し、ＩＤ(b)を得る。こうして得られたＲａ、Ｒｂ、ＩＤ(b)の内、ＲｂおよびＩＤ(b)が、Ｂが送信したものと一致するか検証する。この検証に通った場合、ＢはＡを正当なものとして認証する。

【００７５】次にＢは、認証後に使用するセッション鍵（Session Key（以下、Ｋｓｅｓとする））を生成する（生成方法は、乱数を用いる）。そして、Ｒｂ、Ｒａ、Ｋｓｅｓの順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いて暗号化し、Ａに返送する。

【００７６】これを受信したＡは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、Ｂの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたＲｂ、Ｒａ、Ｋｓｅｓの内、ＲｂおよびＲａが、Ａが送信したものと一致するか検証する。この検証に通った場合、ＡはＢを正当なものとして認証する。互いに相手を認証した後には、セッション鍵Ｋｓｅｓは、認証後の秘密通信のための共通鍵として利用される。

【００７７】なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【００７８】次に、公開鍵暗号方式である１６０ビット長の楕円曲線暗号を用いた相互認証方法を、図１３を用いて説明する。図１３において、公開鍵暗号方式としてＥＣＣを用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも１６０ビットでなくてもよい。図１３において、まずＢが、６４ビットの乱数Ｒｂを生成し、Ａに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａおよび標数ｐより小さい乱数Ａｋを生成する。そして、ベースポイントＧをＡｋ倍した点Ａｖ＝Ａｋ×Ｇを求め、Ｒａ、Ｒｂ、Ａｖ（X座標とY座標）に対する電子署名Ａ．Ｓｉｇ

を生成し、Aの公開鍵証明書とともにBに返送する。ここで、RaおよびRbはそれぞれ64ビット、AvのX座標とY座標がそれぞれ160ビットであるので、合計448ビットに対する電子署名を生成する。

【0079】公開鍵証明書を利用する際には、利用者は自己が保持する公開鍵証明書発行局（CA）410の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の公開鍵証明書発行局（CA）の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図11で説明したのでその詳細は省略する。

【0080】Aの公開鍵証明書、Ra、Rb、Av、電子署名A.Sigを受信したBは、Aが送信してきたRbが、Bが生成したものと一致するか検証する。その結果、一致していた場合には、Aの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Aの公開鍵を取り出す。そして、取り出したAの公開鍵を用い電子署名A.Sigを検証する。電子署名の検証に成功した後、BはAを正当なものとして認証する。

【0081】次に、Bは、標数pより小さい乱数Bkを生成する。そして、ベースポイントGをBk倍した点Bv＝Bk×Gを求め、Rb、Ra、Bv（X座標とY座標）に対する電子署名B.Sigを生成し、Bの公開鍵証明書とともにAに返送する。

【0082】Bの公開鍵証明書、Rb、Ra、Bv、電子署名B.Sigを受信したAは、Bが送信してきたRaが、Aが生成したものと一致するか検証する。その結果、一致していた場合には、Bの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Bの公開鍵を取り出す。そして、取り出したBの公開鍵を用い電子署名B.Sigを検証する。電子署名の検証に成功した後、AはBを正当なものとして認証する。

【0083】両者が認証に成功した場合には、BはBk×Av（Bkは乱数だが、Avは楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、AはAk×Bvを計算し、これら点のX座標の下位64ビットをセッション鍵として以降の通信に使用する（共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合）。もちろん、Y座標からセッション鍵を生成してもよいし、下位64ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

【0084】電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0085】このような相互認証処理において、生成したセッション鍵を用いて、送信データを暗号化して、相互にデータ通信を実行する。

【0086】（2）トランザクションID、購入要求データ生成、および

（3）購入要求データ送信

上述のショップサーバ100とユーザ機器200間の相互認証が成功すると、ユーザ機器200は、コンテンツの購入要求データを生成する。購入要求データの構成を図14（a）に示す。購入要求データは、コンテンツ購入の要求先であるショップサーバ100の識別子であるショップID、コンテンツ取り引きの識別子として、ユーザ機器200の暗号処理手段が例えば乱数に基づいて生成するトランザクションID、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツIDの各データを有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、購入要求データには、ユーザ機器の公開鍵証明書が添付され、ショップサーバ100に送付される。なお、公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ショップ側に送付済みの場合は、必ずしも改めて送付する必要はない。

【0087】（4）受信データ検証

図14（a）に示す購入要求データをユーザ機器200から受信したショップサーバ100は、受信データの検証処理を実行する。検証処理の詳細について図15を用いて説明する。まず、ショップサーバ100は、受信データ中のユーザ機器の公開鍵証明書Cert_DEVの検証（S51）を行なう。これは前述したように、公開鍵証明書に含まれる発行局（CA）の署名を検証する処理（図11参照）として実行され、発行局の公開鍵：KpCAを適用して実行される。

【0088】検証がOK、すなわち公開鍵証明書の改竄がないと判定（S52でYes）されると、S53に進む。検証が非成立の場合（S52でNo）は、S57で公開鍵証明書に改竄ありと判定され、その公開鍵証明書を利用した処理が中止される。S53では、公開鍵証明書からユーザ機器の公開鍵：KpDEVが取り出され、ステップS54で公開鍵：KpDEVを用いた購入要求データのユーザ機器署名の検証処理（図11参照）が実行される。検証がOK、すなわち購入要求データの改竄がないと判定（S55でYes）されると、S56に進み受信データが正当なコンテンツ購入要求データであると判定される。検証が非成立の場合（S55でNo）は、S57で購入要求データが改竄ありと判定され、その購入要求データに対する処理が中止される。

【0089】（5）暗号化コンテンツおよび暗号化コンテンツ鍵データ1（ショップ）送信

ショップサーバ100において、購入要求データの検証が完了し、データ改竄のない正当なコンテンツ購入要求であると判定すると、ショップサーバ100は、暗号化コンテンツおよび暗号化コンテンツ鍵データ1（ショッ

プ）をユーザ機器に送信する。これらは、いずれもコンテンツデータベース１１０に格納されたデータであり、コンテンツをコンテンツキーで暗号化した暗号化コンテンツ：Ｋｃ（content）と、コンテンツキー：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）３００の公開鍵で暗号化した暗号化コンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）である。

【００９０】暗号化コンテンツ鍵データ１（ショップ）の構成を図１４（ｂ）に示す。暗号化コンテンツ鍵データ１（ショップ）は、コンテンツ購入の要求元であるユーザ機器２００の識別子であるユーザ機器ＩＤ、購入要求データ（図１４（ａ）のユーザ機器公開鍵証明書を除いたデータ）、コンテンツ取り引きに伴いショップサーバ１００が生成したショップ処理Ｎｏ．、暗号化コンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）を有し、これらのデータに対するショップサーバ１００の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ１（ショップ）には、ショップサーバ１００の公開鍵証明書が添付され、ユーザ機器２００に送付される。なお、ショップサーバ公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ユーザ機器側に送付済みの場合は、必ずしも改めて送付する必要はない。

【００９１】（６）受信データ検証

ショップサーバ１００から暗号化コンテンツ：Ｋｃ（content）と、図１４（ｂ）に示す暗号化コンテンツ鍵データ１（ショップ）を受信したユーザ機器２００は、暗号化コンテンツ鍵データ１（ショップ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器２００は、まずショップサーバ１００から受領したショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵ＫｐＳＨＯＰを用いて図１４（ｂ）に示す暗号化コンテンツ鍵データ１（ショップ）のショップ署名の検証を実行する。

【００９２】（７）相互認証

ユーザ機器２００が、ショップサーバ１００から暗号化コンテンツ：Ｋｃ（content）と暗号化コンテンツ鍵データ１（ショップ）を受信し、暗号化コンテンツ鍵データ１（ショップ）の検証を終えると、ユーザ機器２００は、ユーザ機器認証サーバ３００にアクセスし、ユーザ機器２００と、ユーザ機器認証サーバ３００間において相互認証処理を実行する。この処理は、前述のショップサーバ１００とユーザ機器２００間の相互認証処理と同様の手続きで実行される。

【００９３】（８）暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求送信

ユーザ機器２００とユーザ機器認証サーバ３００との間の相互認証が成立すると、ユーザ機器２００は、ユーザ機器認証サーバ３００に対して、先にショップサーバ１００から受信した暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を含む暗号化コンテンツ鍵データ（ユーザ機器）と、暗号化コンテンツ鍵かけかえ要求を送信する。

【００９４】暗号化コンテンツ鍵データ（ユーザ機器）の構成を図１４（ｃ）に示す。暗号化コンテンツ鍵データ（ユーザ機器）は、暗号化コンテンツ鍵かけかえ要求の要求先であるユーザ機器認証サーバ３００の識別子であるユーザ機器認証サーバＩＤ、ショップサーバ１００から受領した暗号化コンテンツ鍵データ（図１４（ｂ）のショップ公開鍵証明書を除いたデータ）、を有し、これらのデータに対するユーザ機器２００の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ（ユーザ機器）には、ショップサーバ１００の公開鍵証明書と、ユーザ機器２００の公開鍵証明書が添付され、ユーザ機器認証サーバ３００に送付される。なお、ユーザ機器認証サーバ３００がユーザ機器公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【００９５】（９）受信データ検証

ユーザ機器２００から暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求（図１４（ｃ））を受信したユーザ機器認証サーバ３００は、暗号化コンテンツ鍵かけかえ要求の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器認証サーバ３００は、まずユーザ機器２００から受領したユーザ機器の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器の公開鍵ＫｐＤＥＶを用いて、図１４（ａ）に示す購入要求データおよび図１４（ｃ）に示す暗号化コンテンツ鍵データ（ユーザ機器）の電子署名の検証を実行する。さらに、ショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵ＫｐＳＨＯＰを用いて図１４（ｃ）に示す暗号化コンテンツ鍵データ（ユーザ機器）に含まれる（５）暗号化コンテンツ鍵データ１のショップ署名の検証を実行する。

【００９６】（１０）暗号化コンテンツ鍵かけかえ処理、ユーザ機器認証サーバ３００において、ユーザ機器２００から受信した暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求の検証が終了し、正当な鍵かけかえ要求であると判定すると、ユーザ機器認証サーバ３００は、暗号化コンテンツ鍵データ（ユーザ機器）に含まれる暗号化コンテンツ鍵、すなわち、コンテンツ鍵：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）３００の公開鍵ＫｐＤＡＳで暗号化したデータ：ＫｐＤＡＳ（Ｋｃ）をユーザ機器認証サーバ３００の秘密鍵ＫｓＤＡＳで復号してコンテンツ鍵Ｋｃを取得し、さらにコンテンツ鍵Ｋｃをユーザ機器の公開鍵：ＫｐＤＥＶで暗号化した暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋ

ｃ）を生成する。すなわち、ＫｐＤＡＳ（Ｋｃ）→Ｋｃ→ＫｐＤＥＶ（Ｋｃ）の鍵かけかえ処理を実行する。

【００９７】図１６にユーザ機器認証サーバ３００において実行される暗号化コンテンツ鍵かけかえ処理のフローを示す。まず、ユーザ機器認証サーバ３００は、ユーザ機器２００から受信した暗号化コンテンツ鍵データ（ユーザ機器）から、ユーザ機器認証サーバ（ＤＡＳ）３００の公開鍵ＫｐＤＡＳで暗号化したコンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）を取り出す（Ｓ６１）。次に、ユーザ機器認証サーバ３００の秘密鍵ＫｓＤＡＳで復号してコンテンツ鍵Ｋｃを取得（Ｓ６２）する。次に、復号により取得したコンテンツ鍵Ｋｃをユーザ機器の公開鍵：ＫｐＤＥＶで再暗号化して暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を生成する（Ｓ６３）。これらの処理が終了すると、ライセンス管理データベース（図６参照）のステータスを「鍵かけかえ完了」に設定する。

【００９８】（１１）相互認証

ユーザ機器認証サーバ３００において、上述の暗号化コンテンツ鍵の鍵かけかえ処理が完了すると、ユーザ機器認証サーバ３００は、ショップサーバ１００にアクセスし、ユーザ機器認証サーバ３００とショップサーバ１００間において相互認証処理を実行する。この処理は、前述のショップサーバ１００とユーザ機器２００間の相互認証処理と同様の手続きで実行される。

【００９９】（１２）暗号化コンテンツデータ送信

ユーザ機器認証サーバ３００とショップサーバ１００間の相互認証が成立すると、ユーザ機器認証サーバ３００は、暗号化コンテンツ鍵データ（ＤＡＳ）をショップサーバ１００に送信する。

【０１００】暗号化コンテンツ鍵データ（ＤＡＳ）の構成を図１７（ｄ）に示す。暗号化コンテンツ鍵データ（ＤＡＳ）は、コンテンツ購入の要求先であるショップサーバ１００の識別子であるショップＩＤ、暗号化コンテンツ鍵データ（ユーザ機器）（図１４（ｃ）のショップおよびユーザ機器公開鍵証明書を除いたデータ）、さらに、前述の鍵かけかえ処理により、ユーザ機器認証サーバ３００が生成した暗号化コンテンツ鍵データ：ＫｐＤＥＶ（Ｋｃ）を有し、これらのデータに対するユーザ機器認証サーバ３００の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ（ＤＡＳ）には、ユーザ機器認証サーバ３００と、ユーザ機器２００の公開鍵証明書が添付され、ショップサーバ１００に送付される。なお、ショップサーバが、これらの公開鍵証明書を既に保有済みである場合は、必ずしも改めて送付する必要はない。

【０１０１】また、ユーザ機器認証サーバ３００が信頼できる第三者機関であると認められる存在である場合は、暗号化コンテンツ鍵データ（ＤＡＳ）は、図１７（ｄ）に示すようにユーザ機器の生成した（８）暗号化コンテンツ鍵データ（ユーザ機器）をそのまま含むデータ構成とすることなく、図１８（ｄ’）に示すように、ユーザ機器ＩＤ、トランザクションＩＤ、コンテンツＩＤ、ショップ処理ＮＯ、ユーザデバイスの公開鍵で暗号化したコンテンツ鍵ＫｐＤＥＶ（Ｋｃ）の各データを、ユーザ機器認証サーバ３００が抽出して、これらに署名を付加して暗号化コンテンツ鍵データ（ＤＡＳ）としてもよい。この場合は、（８）暗号化コンテンツ鍵データ（ユーザ機器）の検証が不要となるので、添付する公開鍵証明書は、ユーザ機器認証サーバ３００の公開鍵証明書のみでよい。

【０１０２】（１３）受信データ検証

ユーザ機器認証サーバ３００から暗号化コンテンツ鍵データ（ＤＡＳ）（図１７（ｄ））を受信したショップサーバ１００は、暗号化コンテンツ鍵データ（ＤＡＳ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ショップサーバ１００は、まずユーザ機器認証サーバ３００から受領したユーザ機器認証サーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ３００の公開鍵ＫｐＤＡＳを用いて図１７（ｄ）に示す暗号化コンテンツ鍵データ（ＤＡＳ）の電子署名の検証を実行する。さらに、ユーザ機器の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器の公開鍵ＫｐＤＥＶを用いて図１７（ｄ）に示す暗号化コンテンツ鍵データ（ＤＡＳ）に含まれる（８）暗号化コンテンツ鍵データ（ユーザ機器）のユーザ機器署名の検証を実行する。さらに、また、自己の公開鍵ＫｐＳＨＯＰを用いて、暗号化コンテンツデータ（ユーザ機器）を検証するようにしてもよい。

【０１０３】なお、先に説明した図１８（ｄ’）の簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）をショップサーバ１００が受領した場合は、ショップサーバ１００は、ユーザ機器認証サーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ３００の公開鍵ＫｐＤＡＳを用いて図１８（ｄ’）に示す暗号化コンテンツ鍵データ（ＤＡＳ）の電子署名の検証を実行するのみの処理となる。

【０１０４】（１４）相互認証、および

（１５）暗号化コンテンツ鍵要求データ送信

次に、ユーザ機器２００は、暗号化コンテンツ鍵要求データをショップサーバ１００に対して送信する。なお、この際、前の要求と異なるセッションで要求を実行する場合は、再度相互認証を実行して、相互認証が成立したことを条件として暗号化コンテンツ鍵要求データがユーザ機器２００からショップサーバ１００に送信される。

【０１０５】暗号化コンテンツ鍵要求データの構成を図

１７（ｅ）に示す。暗号化コンテンツ鍵要求データは、コンテンツ購入の要求先であるショップサーバ１００の識別子であるショップＩＤ、先にユーザ機器２００が生成したコンテンツ取り引きの識別子であるトランザクションＩＤ、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツＩＤ、さらに、先にショップが生成し暗号化コンテンツ鍵データ１（ショップ）としてユーザ機器２００に送信してきたデータ（図１４（ｂ）参照）中に含まれるショップ処理Ｎｏ．を有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、暗号化コンテンツ鍵要求データには、ユーザ機器の公開鍵証明書が添付され、ショップサーバ１００に送付される。なお、公開鍵証明書が既にショップ側に保管済みの場合は、必ずしも改めて送付する必要はない。

【０１０６】（１６）検証処理、および
（１７）課金処理

暗号化コンテンツ鍵要求データをユーザ機器から受信したショップサーバ１００は、暗号化コンテンツ鍵要求データの検証処理を実行する。これは、図１５を用いて説明したと同様の処理である。データ検証が済むと、ショップサーバ１００は、コンテンツの取り引きに関する課金処理を実行する。課金処理は、ユーザの取り引き口座からコンテンツ料金を受領する処理である。受領したコンテンツ料金は、コンテンツの著作権者、ショップ、ユーザ機器認証サーバ管理者など、様々な関係者に配分される。

【０１０７】この課金処理に至るまでには、ユーザ機器認証サーバ３００による暗号化コンテンツ鍵の鍵かけかえ処理プロセスが必須となっているので、ショップサーバ１００は、ユーザ機器間とのみの処理では課金処理が実行できない。また、ユーザ機器２００においても暗号化コンテンツ鍵の復号ができないので、コンテンツの利用ができない。ユーザ機器認証サーバは、図６を用いて説明したユーザ機器認証サーバ・ライセンス管理データベースに、すべての鍵かけかえ処理を実行したコンテンツ取り引き内容を記録しており、すべての課金対象となるコンテンツ取り引きが把握可能となる。従って、ショップ側単独でのコンテンツ取り引きは不可能となり、不正なコンテンツ販売が防止される。

【０１０８】（１８）暗号化コンテンツ鍵データ２（ショップ）送信

ショップサーバ１００における課金処理が終了すると、ショップサーバ１００は、暗号化コンテンツ鍵データ２（ショップ）をユーザ機器２００に送信する。

【０１０９】暗号化コンテンツ鍵データ２（ショップ）の構成を図１７（ｆ）に示す。暗号化コンテンツ鍵データ２（ショップ）は、暗号化コンテンツ鍵要求の要求元であるユーザ機器２００の識別子であるユーザ機器ＩＤ、ユーザ機器認証サーバ３００から受領した暗号化コンテンツ鍵データ（ＤＡＳ）（図１７（ｄ）のユーザ機器、ユーザ機器認証サーバ公開鍵証明書を除いたデータ）、を有し、これらのデータに対するショップサーバ１００の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ２（ショップ）には、ショップサーバ１００の公開鍵証明書と、ユーザ機器認証サーバ３００の公開鍵証明書が添付され、ユーザ機器２００に送付される。なお、ユーザ機器２００がユーザ機器認証サーバ公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【０１１０】なお、ユーザ機器認証サーバ３００が信頼できる第三者機関であると認められる存在であり、ショップサーバ１００がユーザ機器認証サーバ３００から受信する暗号化コンテンツ鍵データ（ＤＡＳ）が先に説明した図１８（ｄ’）の簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）である場合は、ショップサーバ１００は、図１８（ｆ’）に示す暗号化コンテンツ鍵データ２（ショップ）をユーザ機器に送付する。すなわち、図１８（ｄ’）に示す簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）にショップサーバの署名を付加したデータに、ショップサーバ１００の公開鍵証明書と、ユーザ機器認証サーバ３００の公開鍵証明書を添付してユーザ機器２００に送付する。

【０１１１】（１９）受信データ検証

ショップサーバ１００から、暗号化コンテンツ鍵データ２（ショップ）を受領したユーザ機器２００は、暗号化コンテンツ鍵データ２（ショップ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器２００は、まずショップサーバ１００から受領したショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバ１００の公開鍵ＫｐＳＨＯＰを用いて図１７（ｆ）に示す暗号化コンテンツ鍵データ２（ショップ）の電子署名の検証を実行する。さらに、ユーザ機器認証サーバ３００の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ３００の公開鍵ＫｐＤＡＳを用いて図１７（ｆ）に示す暗号化コンテンツ鍵データ２（ショップ）に含まれる（１２）暗号化コンテンツ鍵データ（ＤＡＳ）の署名検証を実行する。さらにまた、自己の公開鍵ＫｐＤＥＶを用いて、暗号化コンテンツデータ（ユーザ機器）を検証するようにしてもよい。

【０１１２】（２０）保存処理

ショップサーバ１００から受信した暗号化コンテンツ鍵データ２（ショップ）を検証したユーザ機器２００は、暗号化コンテンツ鍵データ２（ショップ）に含まれる自己の公開鍵ＫｐＤＥＶで暗号化された暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を自己の秘密鍵ＫｓＤＥＶを用

いて復号し、さらに、ユーザ機器の保存鍵Ｋｓｔｏを用いて暗号化して暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を生成して、これをユーザ機器２００の記憶手段に格納する。コンテンツの利用時には、暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を保存鍵Ｋｓｔｏを用いて復号してコンテンツ鍵Ｋｃを取り出して、取り出したコンテンツ鍵Ｋｃを用いて、暗号化コンテンツＫｃ（Content）の復号処理を実行し、コンテンツ（Content）を再生、実行する。

【０１１３】ユーザ機器２００におけるコンテンツ鍵Ｋｃの取得と保存処理フローを図１９に示す。ユーザ機器２００は、まず、ショップサーバ１００から受信した暗号化コンテンツ鍵データ２（ショップ）から自己の公開鍵ＫｐＤＥＶで暗号化された暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を取り出し（Ｓ７１）、取り出した暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を自己の秘密鍵ＫｓＤＥＶを用いて復号してコンテンツ鍵Ｋｃを取り出す（Ｓ７２）。さらに、ユーザ機器の保存鍵Ｋｓｔｏを用いてコンテンツ鍵Ｋｃの暗号化処理を実行して暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を生成して、これをユーザ機器２００の記憶手段（内部メモリ）に格納（Ｓ７３）する。

【０１１４】以上の処理により、ユーザ機器は、暗号化コンテンツＫｃ（Content）と、該暗号化コンテンツのコンテンツ鍵Ｋｃを取得することができ、コンテンツを利用することができる。上述の説明から明らかなように、ユーザ機器２００においてコンテンツ利用可能な状態に至るまでには、ユーザ機器認証サーバ３００における暗号化コンテンツ鍵の鍵かけかえ処理プロセスが必須である。従って、ショップサーバ１００は、ユーザ機器２００に対して、ユーザ機器認証サーバ３００に秘密にコンテンツを販売し、コンテンツをユーザ機器において利用可能な状態とすることができない。ユーザ機器認証サーバは、図６を用いて説明したユーザ機器認証サーバ・ライセンス管理データベースに、すべての鍵かけかえ処理を実行したコンテンツ取り引き内容を記録しており、すべてのショップの取り引きの管理がなされ、課金されたコンテンツ取り引きを把握し、ショップの課金処理において受領されたコンテンツ料金を、コンテンツの著作権者、ショップ、ユーザ機器認証サーバ管理者など、様々な関係者に正確に配分することが可能となる。

【０１１５】（各機器におけるステータス遷移）図１に示すショップサーバ１００、ユーザ機器２００、ユーザ認証サーバ（ＤＡＳ）３００は、それぞれコンテンツ取り引きに係る一連の処理において、処理状態を示すステータスに応じて、次の処理を決定する。ステータスは、例えば図３に示すショップサーバの購買管理データベース、図６のユーザ機器認証サーバのライセンス管理データベース、図８のユーザ機器の購入管理データベースにおいて、各コンテンツ取り引き毎に管理される。

【０１１６】まず、ショップサーバ１００のステータス遷移について、図２０を用いて説明する。ショップサーバは、ユーザ機器２００からのコンテンツ購入要求データを受信（図１の処理（３）に対応）することで処理が開始される。ショップサーバ１００は、ユーザ機器２００からの受信データを検証し、検証に成功した場合は、ステータスを「購入受付完了」に設定し、データ検証により正当な購入要求であるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、購入受付処理を所定回数繰り返した後処理を中止し、ステータスを「購入受付失敗」とする。ステータスが「購入受付完了」である場合にのみ次ステップに進む。

【０１１７】ステータスが「購入受付完了」に遷移すると、次に、ショップサーバ１００は、ユーザ機器２００に対して暗号化コンテンツ鍵データ１（ショップ）を送信（図１の処理（５）に対応）し、ユーザ機器からの受信応答（レスポンス）を受領することにより、ステータスを「鍵１配信完了」とする。鍵データ１の送信が成功しなかった場合は、処理を中止するか、あるいは同様の処理、ここでは、鍵データ１の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵１配信失敗」とする。ステータスが「鍵１配信完了」である場合にのみ次ステップに進む。

【０１１８】ステータスが「鍵１配信完了」に遷移した場合、次に、ショップサーバ１００は、ユーザ機器認証サーバ３００から暗号化コンテンツ鍵データ（ＤＡＳ）を受信（図１の処理（１２）に対応）し、データ検証を実行する。検証に成功した場合は、ステータスを「鍵受信完了」に設定し、データ検証により正当な暗号化コンテンツ鍵データ（ＤＡＳ）であるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵受信失敗」とする。ステータスが「鍵受信完了」である場合にのみ次ステップに進む。

【０１１９】ステータスが「鍵受信完了」に遷移した場合、次に、ショップサーバ１００は、ユーザ機器２００から暗号化コンテンツ鍵送信要求データを受信（図１の処理（１５）に対応）し、データ検証を実行する。検証に成功した場合は、ステータスを「暗号化コンテンツ鍵送信要求受付完了」に設定し、データ検証により正当な鍵送信要求データであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵送信要求データの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「暗号化コンテンツ鍵送信要求受付失敗」とする。ステータスが「暗号化コンテンツ鍵送信要求受付完了」である場合にのみ次ステップに進む。

【０１２０】ステータスが「暗号化コンテンツ鍵送信要

求受付完了」に遷移した場合、次に、ショップサーバ１００は、課金処理（図１の処理（１７）に対応）を実行する。課金処理が完了すると、ステータスを「課金完了」に設定し、課金処理が終了しなかった場合、例えばユーザ機器の指定口座からのコンテンツ料金引き落としができなかった場合などには、以降の処理は実行せず、処理を中止するか、あるいは同様の処理、ここでは、課金処理を所定回数繰り返した後、処理を中止し、ステータスを「課金失敗」とする。ステータスが「課金完了」である場合にのみ次ステップに進む。

【０１２１】ステータスが「課金完了」に遷移した場合、次に、ショップサーバ１００は、ユーザ機器へ暗号化コンテンツ鍵データ２（ショップ）送信処理（図１の処理（１８）に対応）を実行する。暗号化コンテンツ鍵データ２（ショップ）送信処理が完了し、ユーザ機器からの受信レスポンスを受信すると、ステータスを「鍵２配信完了」に設定し、鍵データ２（ショップ）送信処理が終了しなかった場合には、ステータスを「鍵２配信失敗」とする。ステータスが「鍵２配信完了」である場合にのみ次ステップ、ここでは処理終了となり、ステータスが「鍵２配信失敗」である場合は、以降の処理は実行せず、処理を中止するか、あるいは同様の処理、ここでは、鍵データ２（ショップ）送信処理を所定回数繰り返す。ショップサーバ１００は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【０１２２】次に、ユーザ機器２００のステータス遷移について、図２１を用いて説明する。ユーザ機器２００は、まず、ショップサーバ１００に対してコンテンツ購入要求データを送信（図１の処理（３）に対応）することで処理が開始される。ユーザ機器２００は、ショップサーバ１００に対するコンテンツ購入要求データの受信完了のレスポンスを受信すると、ステータスを「購入要求送信完了」に設定し、ショップサーバ１００からの受信完了のレスポンスを受信できない場合は、処理を中止するか、あるいは同様の処理、ここでは、購入要求送信処理を所定回数繰り返した後、処理を中止し、ステータスを「購入要求送信失敗」とする。ステータスが「購入要求送信完了」である場合にのみ次ステップに進む。

【０１２３】ステータスが「購入要求送信完了」に遷移すると、次に、ユーザ機器２００は、ショップサーバ１００から、暗号化コンテンツ鍵データ１（シヨップ）を受信（図１の処理（５）に対応）し、受信データを検証する。ショップサーバ１００からの暗号化コンテンツ鍵データの検証に成功した場合は、ステータスを「鍵１受信完了」に設定し、データ検証により正当な暗号化コンテンツ鍵データであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵１受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵１受信失敗」とする。ステータスが「鍵１受信完了」である場合にのみ次ステップに進む。

【０１２４】ステータスが「鍵１受信完了」に遷移した場合、次に、ユーザ機器２００は、ユーザ機器認証サーバ３００に対して、暗号化コンテンツ鍵データ（ユーザ機器）を送信（図１の処理（８）に対応）し、データ受信レスポンスを受信する。データ受信レスポンスを受信した場合は、ステータスを「鍵送信完了」に設定し、データ受信レスポンスを受信しない場合は、処理を中止するか、あるいは同様の処理、ここでは、鍵送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵送信失敗」とする。ステータスが「鍵送信完了」である場合にのみ次ステップに進む。

【０１２５】ステータスが「鍵送信完了」に遷移した場合、次に、ユーザ機器２００は、ショップサーバ１００に対して、暗号化コンテンツ鍵送信要求を送信（図１の処理（１５）に対応）し、データ受信レスポンスを受信する。データ受信レスポンスを受信した場合は、ステータスを「暗号化コンテンツ鍵送信要求送信完了」に設定し、データ受信レスポンスを受信しない場合は、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵送信要求送信処理を所定回数繰り返した後、処理を中止し、ステータスを「暗号化コンテンツ鍵送信要求送信失敗」とする。ステータスが「暗号化コンテンツ鍵送信要求送信完了」である場合にのみ次ステップに進む。

【０１２６】ステータスが「暗号化コンテンツ鍵送信要求送信完了」に遷移した場合、次に、ユーザ機器２００は、ショップサーバ１００から、暗号化コンテンツ鍵データ２（ショップ）を受信（図１の処理（１８）に対応）し、データ検証を行なう。データ検証に成功した場合は、ステータスを「鍵２受信完了」に設定し、データ検証に成功しなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵データ２（ショップ）受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵２受信失敗」とする。ステータスが「鍵２受信完了」である場合には処理終了となる。ユーザ機器２００は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【０１２７】次にユーザ機器認証サーバ３００のステータス遷移について、図２２を用いて説明する。ユーザ機器認証サーバ３００は、ユーザ機器２００からの暗号化コンテンツ鍵データ（ユーザ機器）を受信（図１の処理（８）に対応）することで処理が開始される。ユーザ機器認証サーバ３００は、ユーザ機器２００からの受信データを検証し、検証に成功した場合は、ステータスを「鍵受信完了」に設定し、データ検証により正当なデータであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵データ（ユーザ機器）の受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵受信失

敗」とする。ステータスが「鍵受信完了」である場合にのみ次ステップに進む。

【０１２８】ステータスが「鍵受信完了」に遷移すると、次に、ユーザ機器認証サーバ３００は、コンテンツ鍵かけかえ処理（図１の処理（１０）に対応）を実行し、鍵かけかえ処理が完了した場合には、ステータスを「鍵かけかえ完了」とする。鍵かけかえに失敗することは想定していないので、ここでは「鍵かけかえ完了」のみのステータス遷移が存在する。

【０１２９】ステータスが「鍵かけかえ完了」に遷移した場合、次に、ユーザ機器認証サーバ３００は、ショップサーバ１００に対して暗号化コンテンツ鍵データ（ＤＡＳ）を送信（図１の処理（１２）に対応）し、ショップサーバ１００からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「鍵送信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵データ（ＤＡＳ）の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵送信失敗」とする。ステータスが「鍵送信完了」である場合には、処理終了となる。ユーザ機器認証サーバ３００は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【０１３０】（コンテンツ購入処理フロー）次に、ユーザ機器からショップサーバに対するコンテンツ購入要求に伴ってショップサーバ１００、ユーザ機器２００、ユーザ機器認証サーバ３００間で実行されるデータ送受信処理をフローに従って説明する。処理フローは、以下のＡ，Ｂ，Ｃ，Ｄに分割して説明する。

【０１３１】Ａ．ショップサーバとユーザ機器間における処理（図１に示す（１）～（６）の処理）

ユーザ機器２００とショップサーバ１００の相互認証～ユーザ機器２００からショップサーバ１００に対するコンテンツ購入要求～ショップサーバ１００からユーザ機器２００に対する鍵１（ショップ）の送信。

Ｂ．ユーザ機器認証サーバとユーザ機器間における処理（図１に示す（７）～（９）の処理）

ユーザ機器２００とユーザ機器認証サーバ３００の相互認証～暗号化コンテンツ鍵データ送信～ユーザ機器認証サーバ３００における受信データ検証。

Ｃ．ユーザ機器認証サーバとショップサーバ間における処理（図１に示す（１１）～（１３）の処理）

ユーザ機器認証サーバ３００とショップサーバ１００間の相互認証～暗号化コンテンツ鍵データ（ＤＡＳ）送信～ショップサーバにおける受信データ検証。

Ｄ．ショップサーバとユーザ機器間における処理（図１に示す（１４）～（１９）の処理）

ユーザ機器２００とショップサーバ１００の相互認証～ユーザ機器２００からショップサーバ１００に対する暗号化コンテンツ鍵要求データ送信～ショップサーバ１００からユーザ機器２００に対する鍵２（ショップ）の送信～ユーザ機器２００における受信データ検証。

【０１３２】まず、Ａ．ショップサーバとユーザ機器間における処理（図１に示す（１）～（６）の処理）について、図２３、図２４を用いて説明する。

【０１３３】図２３、図２４において、左側がショップサーバの処理、右側がユーザ機器の処理を示す。なお、すべてのフローにおいて、ショップサーバの処理ステップＮｏをＳ１０ｘｘ、ユーザ機器の処理ステップＮｏをＳ２０ｘｘ、ユーザ機器認証サーバの処理ステップＮｏをＳ３０ｘｘとして示す。

【０１３４】まず、図２３に示すように、処理開始時に、ショップサーバとユーザ機器間において相互認証が実行される（Ｓ１００１，Ｓ２００１）。相互認証処理は、図１２または図１３を用いて説明した処理として実行される。相互認証処理において生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。相互認証が成立すると、ショップサーバは、購買管理データベース（図３参照）に新規ショップ処理ＮＯを新たな処理エントリとして追加（Ｓ１００３）する。

【０１３５】一方、ユーザ機器は、相互認証が成立すると、今回のコンテンツ取り引きにおいて適用するトランザクションＩＤを例えば乱数に基づいて生成し、購入データベース（図８参照）に新規トランザクションＩＤを新たなエントリとして追加（Ｓ２００３）する。さらに、ユーザ機器は、ショップサーバに対するコンテンツ購入要求データの送信（Ｓ２００４）、すなわち、図１４（ａ）に示す（３）購入要求データの送信を実行する。

【０１３６】ショップサーバは、ユーザ機器からのコンテンツ購入要求データを受信（Ｓ１００４）し、受信データ（Ｓ１００５）の検証を実行する。データ検証は、先に説明した図１１の処理フローに従った処理である。受信データの検証により、データが改竄のない正当なデータであると認められると、ユーザ機器に対して受信ＯＫのレスポンスを送信（Ｓ１００８）し、購買管理データベースのステータスを「購入受付完了」に設定（Ｓ１０１０）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ユーザ機器に対して受信ＮＧのレスポンスを送信（Ｓ１００７）し、購買管理データベースのステータスを「購入受付失敗」に設定（Ｓ１００９）する。

【０１３７】ユーザ機器は、ショップサーバからの受信ＯＫのレスポンスを受信（Ｓ２００５，Ｓ２００６でＹｅｓ）すると、購入管理データベースのステータスを「購入要求送信完了」に設定し、ショップサーバからの受信ＮＧレスポンスを受信（Ｓ２００５，Ｓ２００６でＮｏ）すると、購入管理データベースのステータスを「購入要求送信失敗」に設定する。

【０１３８】ショップサーバでは、購買管理データベースのステータスを「購入受付完了」に設定（Ｓ１０１０）後、暗号化コンテンツ鍵データ１（ショップ）（図１４（ｂ）参照）を生成（Ｓ１０１１）し、ユーザ機器に対して、コンテンツ鍵：Ｋｃで暗号化した暗号化コンテンツ：Ｋｃ（Content）を送信（Ｓ１０１２）し、さらに、図１４（ｂ）に示す暗号化コンテンツ鍵データ１（ショップ）を送信（Ｓ１０１３）する。

【０１３９】ユーザ機器は、購入管理データベースのステータスを「購入要求送信完了」に設定（Ｓ２００７）後、ショップサーバから、コンテンツ鍵：Ｋｃで暗号化した暗号化コンテンツ：Ｋｃ（Content）を受信（Ｓ２００９）し、さらに、ショップサーバから暗号化コンテンツ鍵データ１（ショップ）（図１４（ｂ））を受信（Ｓ２０１０）する。

【０１４０】ユーザ機器は、ステップＳ２００９，Ｓ２０１０で受信したデータの検証処理（図１１参照）を実行（Ｓ２０２１）し、受信データの検証により、データが改竄のない正当なデータであると認められると、ショップサーバに対して受信ＯＫのレスポンスを送信（Ｓ２０２３）し、購入管理データベースのステータスを「鍵１受信完了」に設定（Ｓ２０２５）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ショップサーバに対して受信ＮＧのレスポンスを送信（Ｓ２０２４）し、購入管理データベースのステータスを「鍵１受信失敗」に設定（Ｓ２０２６）した後、ショップサーバとの接続を切る（Ｓ２０２７）。

【０１４１】ショップサーバは、ユーザ機器からのレスポンスを受信（Ｓ１０２１）し、レスポンスがＯＫである場合は、購買管理データベースのステータスを「鍵１配信成功」に設定（Ｓ１０２４）する。レスポンスがＮＧである場合は、購買管理データベースのステータスを「鍵１配信失敗」に設定（Ｓ１０２３）した後、ユーザ機器との接続を切る（Ｓ１０２５）。

【０１４２】なお、ステップＳ１００２，Ｓ２００２の相互認証失敗の場合、Ｓ１００９のステータスの「購入受付失敗」の設定、および、Ｓ２００８のステータスの「購入要求送信失敗」の設定の場合は、いずれも処理を中止して、接続を切る処理を行なって処理終了とする。

【０１４３】次に、Ｂ．ユーザ機器認証サーバとユーザ機器間における処理（図１に示す（７）～（９）の処理）について、図２５のフローに従って説明する。

【０１４４】まず、ユーザ機器認証サーバとユーザ機器間において相互認証が実行される（Ｓ３００１，Ｓ２０３１）。相互認証処理は、図１２または図１３を用いて説明した処理として実行される。相互認証処理において生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。相互認証が成立すると、ユーザ機器認証サーバは、ライセンス管理データベース（図６参照）に新規ユーザ機器認証サーバ処理ＮＯ、を新たな処理エントリとして追加（Ｓ３００３）する。

【０１４５】一方、ユーザ機器は、相互認証が成立すると、暗号化コンテンツ鍵データ（ユーザ機器）（図１４（ｃ）参照）を生成（Ｓ２０３３）し、ユーザ機器認証サーバへ送信（Ｓ２０３４）する。

【０１４６】ユーザ機器認証サーバは、ユーザ機器からの暗号化コンテンツ鍵データ（ユーザ機器）を受信（Ｓ３００４）し、受信データの検証（Ｓ３００５）を実行する。データ検証は、先に説明した図１１の処理フローに従った処理である。受信データの検証により、データが改竄のない正当なデータであると認められると、ユーザ機器に対して受信ＯＫのレスポンスを送信（Ｓ３００８）し、ライセンス管理データベースのステータスを「鍵受信完了」に設定（Ｓ３０１０）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ユーザ機器に対して受信ＮＧのレスポンスを送信（Ｓ３００７）し、ライセンス管理データベースのステータスを「鍵受信失敗」に設定（Ｓ３００９）後、ユーザ機器との接続を切る（Ｓ３０１１）。

【０１４７】ユーザ機器は、ユーザ機器認証サーバからの受信ＯＫのレスポンスを受信（Ｓ２０３５，Ｓ２０３６でＹｅｓ）すると、購入管理データベースのステータスを「鍵送信完了」に設定（Ｓ２０３７）し、ユーザ機器認証サーバからの受信ＮＧレスポンスを受信（Ｓ２０３５，Ｓ２０３６でＮｏ）すると、購入管理データベースのステータスを「鍵送信失敗」に設定（Ｓ２０３８）した後、ユーザ機器認証サーバとの接続を切る（Ｓ２０３９）。

【０１４８】なお、ステップＳ３００２，Ｓ２０３２の相互認証失敗の場合は、処理を中止して、接続を切る処理を行なって処理終了とする。

【０１４９】次に、Ｃ．ユーザ機器認証サーバとショップサーバ間における処理（図１に示す（１１）～（１３）の処理）について、図２６のフローに従って説明する。

【０１５０】まず、ユーザ機器認証サーバとショップサーバ間において相互認証が実行される（Ｓ３０２１，Ｓ１０３１）。相互認証処理は、図１２または図１３を用いて説明した処理として実行される。相互認証処理において生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。相互認証が成立すると、ユーザ機器認証サーバは、暗号化コンテンツ鍵データ（ＤＡＳ）（図１７（ｄ）参照）を生成（Ｓ３０２３）し、ショップサーバに送信（Ｓ３０２４）する。

【０１５１】一方、ショップサーバは、相互認証の成立後、ユーザ機器認証サーバから暗号化コンテンツ鍵データ（ＤＡＳ）（図１７（ｄ）参照）を受信（Ｓ１０３

3）し、受信データの検証（Ｓ１０３４）を実行する。データ検証は、先に説明した図１１の処理フローに従った処理である。受信データの検証により、データが改竄のない正当なデータであると認められると、ユーザ機器認証サーバに対して受信ＯＫのレスポンスを送信（Ｓ１０３６）し、購買管理データベースのステータスを「鍵受信完了」に設定（Ｓ１０３８）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ユーザ機器認証サーバに対して受信ＮＧのレスポンスを送信（Ｓ１０３７）し、購買管理データベースのステータスを「鍵受信失敗」に設定（Ｓ１０３９）後、ユーザ機器認証サーバとの接続を切る（Ｓ１０４０）。

【０１５２】ユーザ機器認証サーバは、ショップサーバからの受信ＯＫのレスポンスを受信（Ｓ３０２５，Ｓ３０２６でＹｅｓ）すると、ライセンス管理データベースのステータスを「鍵送信完了」に設定（Ｓ３０２８）し、ショップサーバからの受信ＮＧレスポンスを受信（Ｓ３０２５，Ｓ３０２６でＮｏ）すると、ライセンス管理データベースのステータスを「鍵送信失敗」に設定（Ｓ３０２７）した後、ユーザ機器認証サーバとの接続を切る（Ｓ３０２９）。

【０１５３】なお、ステップＳ３０２２，Ｓ１０３２の相互認証失敗の場合は、処理を中止して、接続を切る処理を行なって処理終了とする。

【０１５４】次に、Ｄ．ショップサーバとユーザ機器間における処理（図１に示す（１４）～（１９）の処理）について、図２７、図２８を用いて説明する。

【０１５５】まず、処理開始時に、ショップサーバとユーザ機器間において相互認証が実行される（Ｓ１０５１，Ｓ２０５１）。相互認証処理は、図１２または図１３を用いて説明した処理として実行される。相互認証処理において生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。相互認証が成立すると、ユーザ機器は、暗号化コンテンツ鍵送信要求データ（図１７（ｅ）参照）を生成（Ｓ２０５３）し、ショップサーバへ送信（Ｓ２０５４）する。

【０１５６】ショップサーバは、ユーザ機器からの暗号化コンテンツ鍵送信要求データを受信（Ｓ１０５４）し、受信データの検証を実行（Ｓ１０５５）する。データ検証は、先に説明した図１１の処理フローに従った処理である。受信データの検証により、データが改竄のない正当なデータであると認められると、ユーザ機器に対して受信ＯＫのレスポンスを送信（Ｓ１０５８）し、購買管理データベースのステータスを「暗号化コンテンツ鍵送信要求受付完了」に設定（Ｓ１０６０）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ユーザ機器に対して受信ＮＧのレスポンスを送信（Ｓ１０５７）し、購買管理データベースのステータスを「暗号化コンテンツ鍵送信要求受付失敗」に設定（Ｓ１０５９）する。

【０１５７】ユーザ機器は、ショップサーバからの受信ＯＫのレスポンスを受信（Ｓ２０５５，Ｓ２０５６でＹｅｓ）すると、購入管理データベースのステータスを「暗号化コンテンツ鍵送信要求送信完了」に設定（Ｓ２０５７）し、ショップサーバからの受信ＮＧレスポンスを受信（Ｓ２０５５，Ｓ２０５６でＮｏ）すると、購入管理データベースのステータスを「暗号化コンテンツ鍵送信要求送信失敗」に設定（Ｓ２０５８）する。

【０１５８】ショップサーバでは、購買管理データベースのステータスを「暗号化コンテンツ鍵送信要求受付完了」に設定（Ｓ１０６０）後、暗号化コンテンツ鍵データ２（ショップ）（図１７（ｆ）参照）を生成（Ｓ１０６１）し、ユーザ機器に対して、図１７（ｆ）に示す暗号化コンテンツ鍵データ２（ショップ）を送信（Ｓ１０６２）する。

【０１５９】ユーザ機器は、購入管理データベースのステータスを「暗号化コンテンツ鍵送信要求送信完了」に設定（Ｓ２０５７）後、ショップサーバから、暗号化コンテンツ鍵データ２（ショップ）（図１７（ｆ））を受信（Ｓ２０５９）する。

【０１６０】ユーザ機器は、ステップＳ２０５９で受信したデータの検証処理（図１１参照）を実行（Ｓ２０７１）し、受信データの検証により、データが改竄のない正当なデータであると認められると、ショップサーバに対して受信ＯＫのレスポンスを送信（Ｓ２０７３）し、購入管理データベースのステータスを「鍵２受信完了」に設定（Ｓ２０７５）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ショップサーバに対して受信ＮＧのレスポンスを送信（Ｓ２０７４）し、購入管理データベースのステータスを「鍵２受信失敗」に設定（Ｓ２０７６）した後、ショップサーバとの接続を切る（Ｓ２０７７）。

【０１６１】ショップサーバは、ユーザ機器からのレスポンスを受信（Ｓ１０７１）し、レスポンスがＯＫである場合は、購買管理データベースのステータスを「鍵２配信成功」に設定（Ｓ１０７４）する。レスポンスがＮＧである場合は、購買管理データベースのステータスを「鍵２配信失敗」に設定（Ｓ１０７３）した後、ユーザ機器との接続を切る（Ｓ１０７５）。

【０１６２】なお、ステップＳ１０５２，Ｓ２０５２の相互認証失敗の場合は、処理を中止して、接続を切る処理を行なって処理終了とする。

【０１６３】［基本コンテンツ配信モデル１の変形例］ここまで、図１に示した基本コンテンツ配信モデル１の構成に基づいてコンテンツ購入処理の構成、処理手順について説明してきたが、基本的にユーザ機器認証サーバにおいてコンテンツ鍵のかけかえ処理を実行する構成とするポリシーを持つ構成であれば、図１に示す構成に限らず、様々な態様が実現可能である。以下、様々な変形

例について説明する。

【０１６４】図２９に示す構成は、ショップサーバの機能を分離し、ショップサーバと配信サーバを設けた構成である。ショップサーバ１００は、ユーザ機器２００からのコンテンツ購入要求を受領するが、ユーザ機器２００に対するコンテンツ配信は配信サーバ４００が実行する。本例では、各エンティテイ間で相互認証処理を省略しているが、基本コンテンツ配信モデル１同様、相互認証処理を行なっても構わない。

【０１６５】ショップサーバ１００は、ユーザ機器２００からの購入要求データを受信し、データの検証（図２９の処理（３））を行なって、要求データの正当性を確認した後、配信サーバ４００に対して、コンテンツ配信要求の送信を実行（図２９の処理（４））する。配信サーバ４００は、ショップサーバ１００からのコンテンツ配信要求データを検証し、データの正当性が確認された場合、コンテンツデータベース４１０から取り出した暗号化コンテンツおよび暗号化コンテンツ鍵データ（配信サーバ）を送信（図２９の処理（６））する。暗号化コンテンツ鍵データ（配信サーバ）は、前述の実施例の暗号化コンテンツ鍵データ１（ショップ）に対応し、ユーザ機器認証サーバの公開鍵ＫｐＤＡＳで暗号化したコンテンツ鍵Ｋｃ、すなわちＫｐＤＡＳ（Ｋｃ）を含むデータである。

【０１６６】ユーザ機器２００が配信サーバ４００から暗号化コンテンツおよび暗号化コンテンツ鍵データ（配信サーバ）を受信した以後の処理は、先の図１に示した構成に基づく実施例と同様となる。

【０１６７】本構成においては、ショップサーバ１００は、ユーザ機器からのコンテンツ要求を受け付けて、その正当性を検証する機能、ユーザ機器認証サーバからの、かけかえ済みの暗号化コンテンツ鍵を受信し、ユーザ機器に対する配信を主として実行し、コンテンツ自体の管理、配信を行なわない。従って、例えば音楽データを管理する音楽コンテンツ配信サーバ、ゲームコンテンツを管理するゲームコンテンツ配信サーバ等、様々なコンテンツ管理主体となる複数の配信サーバに対して１つのショップサーバがユーザ機器からのコンテンツ要求に応答し、ショップサーバが要求に応じて要求コンテンツを管理する配信サーバにコンテンツ配信要求を送信する構成に適した態様である。また、この構成にしたことにより、例えば、ユーザ機器とショップサーバは双方向通信であるため、インターネットを使うが、配信サーバからユーザ機器へは片方向通信であるため、高速な衛星通信が利用できるメリットがある。

【０１６８】図３０は、図２９と同様ショップサーバの機能を分離し、ショップサーバと配信サーバを設けた構成であり、ショップサーバ１００は、ユーザ機器２００からのコンテンツ購入要求を受領するが、ユーザ機器２００に対するコンテンツ配信は配信サーバ４００が実行する。図２９の構成と異なる点は、ショップサーバ１００から配信サーバ４００に対してコンテンツ配信要求を送信せず、ユーザ機器認証サーバ３００が、配信サーバ４００に対してコンテンツ配信要求を送信する構成とした点である。

【０１６９】ショップサーバ１００は、ユーザ機器２００からの購入要求データを受信し、データの検証（図３０の処理（３））を行なって、要求データの正当性を確認した後、ユーザ機器認証サーバ３００に対して、コンテンツ配信要求の送信を実行（図３０の処理（４））する。その後、ユーザ機器認証サーバ３００は、データの検証（図３０の処理（５））を行なって、要求データの正当性を確認した後、配信サーバ４００に対して、コンテンツ配信要求の送信を実行（図３０の処理（６））する。配信サーバ４００は、ユーザ機器認証サーバ３００からのコンテンツ配信要求データを検証し、正当性が確認された場合、ユーザ機器２００に対して、コンテンツデータベース４１０から取り出した暗号化コンテンツおよび暗号化コンテンツ鍵データ（配信サーバ）を送信（図３０の処理（８））する。暗号化コンテンツ鍵データ（配信サーバ）は、前述の実施例の暗号化コンテンツ鍵データ１（ショップ）に対応し、ユーザ機器認証サーバの公開鍵ＫｐＤＡＳで暗号化したコンテンツ鍵Ｋｃ、すなわちＫｐＤＡＳ（Ｋｃ）を含むデータである。

【０１７０】ユーザ機器２００が配信サーバ４００から暗号化コンテンツおよび暗号化コンテンツ鍵データ（配信サーバ）を受信した以後の処理は、先の図１に示した構成に基づく実施例と同様となる。

【０１７１】本構成においては、ユーザ機器認証サーバ３００は、ユーザ機器２００からの鍵のかけかえ要求以前、ショップサーバ１００に対してコンテンツ購入要求があった時点で、コンテンツ購入要求主体であるユーザ機器情報を取得し、管理することが可能となる。従って、ユーザ機器２００からの鍵のかけかえ要求受領時に、すでに登録済みのコンテンツ購入要求ユーザ機器であるか否かの照合処理が可能となる。

【０１７２】［１．３．基本コンテンツ配信モデル２］

次に、図３１を用いて基本コンテンツ配信モデル１と異なる基本コンテンツ配信モデル２について説明する。基本コンテンツ配信モデル２では、ユーザ機器２００とユーザ機器認証サーバ３００との間ではデータ送受信が行われない。図３１に示す各処理（１）～（１９）について、基本コンテンツ配信モデル１との相違点を中心に説明する。なお、本実施例では、エンティテイ間の通信において相互認証処理（（１）、（７）、（１３））を行なったものを述べているが、必要に応じて省略しても構わない。

【０１７３】（１）相互認証

コンテンツをショップサーバ１００から購入しようとするユーザ機器２００は、ショップサーバ１００との間で

相互認証処理を行なう。相互認証処理は、図１２または図１３を用いて説明した処理である。相互認証処理において、生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。

【０１７４】（２）トランザクションＩＤ、購入要求データ生成、および

（３）購入要求データ送信

ショップサーバ１００とユーザ機器２００間の相互認証が成功すると、ユーザ機器２００は、コンテンツの購入要求データを生成する。購入要求データの構成を図３２（ｇ）に示す。購入要求データは、コンテンツ購入の要求先であるショップサーバ１００の識別子であるショップＩＤ、コンテンツ取り引きの識別子として、ユーザ機器２００の暗号処理手段が乱数に基づいて生成するトランザクションＩＤ、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツＩＤの各データを有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、購入要求データには、ユーザ機器の公開鍵証明書が添付され、ショップサーバ１００に送付される。なお、公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ショップ側に送付済みの場合は、必ずしも改めて送付する必要はない。

【０１７５】（４）受信データ検証

図３２（ｇ）に示す購入要求データをユーザ機器２００から受信したショップサーバ１００は、受信データの検証処理を実行する。検証処理の詳細は、先に図１５を用いて説明した通りである。

【０１７６】（５）暗号化コンテンツおよび購入受付データ送信

ショップサーバ１００において、購入要求データの検証が完了し、データ改竄のない正当なコンテンツ購入要求であると判定すると、ショップサーバ１００は、暗号化コンテンツおよび購入受付データをユーザ機器に送信する。これらは、コンテンツをコンテンツキーで暗号化した暗号化コンテンツ：Ｋｃ（content）と、購入要求を受け付けたことを示すのみのデータであり、先のコンテンツキー：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）３００の公開鍵で暗号化した暗号化コンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）を含まないデータである。

【０１７７】購入受付データの構成を図３２（ｈ）に示す。購入受付データは、コンテンツ購入の要求元であるユーザ機器２００の識別子であるユーザ機器ＩＤ、購入要求データ（図３２（ｇ）のユーザ機器公開鍵証明書を除いたデータ）、コンテンツ取り引きに伴いショップサーバ１００が生成したショップ処理Ｎｏ．を有し、これらのデータに対するショップサーバ１００の電子署名が付加されている。さらに、購入受付データには、ショップサーバ１００の公開鍵証明書が添付され、ユーザ機器２００に送付される。なお、ショップサーバ公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ユーザ機器側に送付済みの場合は、必ずしも改めて送付する必要はない。

【０１７８】（６）受信データ検証

ショップサーバ１００から暗号化コンテンツ：Ｋｃ（content）と、図３２（ｈ）に示す購入受付データを受信したユーザ機器２００は、購入受付データの検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器２００は、まずショップサーバ１００から受領したショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵ＫｐＳＨＯＰを用いて図３２（ｈ）に示す購入受付データのショップ署名の検証を実行する。

【０１７９】（７）相互認証

（８）暗号化コンテンツ鍵データ１（ショップ）送信

次にショップサーバ１００は、ユーザ機器認証サーバ３００にアクセスし、ショップサーバ１００と、ユーザ機器認証サーバ３００間において相互認証処理を実行する。相互認証が成立すると、ショップサーバ１００は、ユーザ機器認証サーバ３００に対して、暗号化コンテンツ鍵データ１（ショップ）を送信する。

【０１８０】暗号化コンテンツ鍵データ１（ショップ）の構成を図３２（ｉ）に示す。暗号化コンテンツ鍵データ１（ショップ）は、暗号化コンテンツ鍵かけかえ要求の要求先であるユーザ機器認証サーバ３００の識別子であるユーザ機器認証サーバＩＤ、ユーザ機器２００から受領した購入要求データ（図３２（ｇ）のユーザ機器公開鍵証明書を除いたデータ）、ショップ処理Ｎｏ．を有し、これらのデータに対するショップサーバ１００の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ１（ショップ）には、ショップサーバ１００の公開鍵証明書と、ユーザ機器２００の公開鍵証明書が添付され、ユーザ機器認証サーバ３００に送付される。なお、ユーザ機器認証サーバ３００がユーザ機器公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【０１８１】（９）受信データ検証

ショップサーバ１００から暗号化コンテンツ鍵データ１（ショップ）（図３２（ｉ））を受信したユーザ機器認証サーバ３００は、受信データの検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器認証サーバ３００は、まずショップサーバ１００から受領したショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵ＫｐＳＨＯＰを用いて図３２（ｉ）に示す暗号化コンテンツ鍵データ１（ショップ）の電子署名の検証を実行する。さらに、ユーザ機器の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実

行し、次に公開鍵証明書から取り出したユーザ機器の公開鍵ＫｐＤＥＶを用いて図３２（ｉ）に示す暗号化コンテンツ鍵データ１（ショップ）に含まれる（３）購入要求データのユーザ機器署名の検証を実行する。

【０１８２】（１０）暗号化コンテンツ鍵かけかえ処理

ユーザ機器認証サーバ３００において、ショップサーバ１００から受信した暗号化コンテンツ鍵データ１（ショップ）の検証が終了し、正当なデータであると判定すると、ユーザ機器認証サーバ３００は、暗号化コンテンツ鍵データ１（ショップ）に含まれる暗号化コンテンツ鍵、すなわち、コンテンツ鍵：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）３００の公開鍵ＫｐＤＡＳで暗号化したデータ：ＫｐＤＡＳ（Ｋｃ）をユーザ機器認証サーバ３００の秘密鍵ＫｓＤＡＳで復号してコンテンツ鍵Ｋｃを取得し、さらにコンテンツ鍵Ｋｃをユーザ機器の公開鍵：ＫｐＤＥＶで暗号化した暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を生成する。すなわち、ＫｐＤＡＳ（Ｋｃ）→Ｋｃ→ＫｐＤＥＶ（Ｋｃ）の鍵かけかえ処理を実行する。この処理は、先に説明した図１６に示すフローに従った処理である。

【０１８３】（１１）暗号化コンテンツデータ送信

次に、ユーザ機器認証サーバ３００は、暗号化コンテンツ鍵データ（ＤＡＳ）をショップサーバ１００に送信する。

【０１８４】暗号化コンテンツ鍵データ（ＤＡＳ）の構成を図３３（ｊ）に示す。暗号化コンテンツ鍵データ（ＤＡＳ）は、コンテンツ購入の要求先であるショップサーバ１００の識別子であるショップＩＤ、暗号化コンテンツ鍵データ１（ショップ）（図３２（ｉ）のショップおよびユーザ機器公開鍵証明書を除いたデータ）、さらに、前述の鍵かけかえ処理により、ユーザ機器認証サーバ３００が生成した暗号化コンテンツ鍵データ：ＫｐＤＥＶ（Ｋｃ）を有し、これらのデータに対するユーザ機器認証サーバ３００の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ（ＤＡＳ）には、ユーザ機器認証サーバ３００と、ユーザ機器２００の公開鍵証明書が添付され、ショップサーバ１００に送付される。なお、ショップサーバが、これらの公開鍵証明書を既に保有済みである場合は、必ずしも改めて送付する必要はない。

【０１８５】また、ユーザ機器認証サーバ３００が信頼できる第三者機関であると認められる存在である場合は、暗号化コンテンツ鍵データ（ＤＡＳ）は、図３３（ｊ）に示すような（８）暗号化コンテンツ鍵データ１（ショップ）をそのまま含むデータ構成とすることなく、図３４（ｊ’）に示すように、ショップＩＤ、ユーザ機器ＩＤ、トランザクションＩＤ、コンテンツＩＤ、ショップ処理ＮＯ、ユーザデバイスの公開鍵で暗号化したコンテンツ鍵ＫｐＤＥＶ（Ｋｃ）の各データを、ユーザ機器認証サーバ３００が抽出して、これらに署名を付加して暗号化コンテンツ鍵データ（ＤＡＳ）としてもよい。添付する公開鍵証明書は、ユーザ機器認証サーバ３００の公開鍵証明書である。

【０１８６】（１２）受信データ検証

ユーザ機器認証サーバ３００から暗号化コンテンツ鍵データ（ＤＡＳ）（図３３（ｊ））を受信したショップサーバ１００は、暗号化コンテンツ鍵データ（ＤＡＳ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ショップサーバ１００は、まずユーザ機器認証サーバ３００から受領したユーザ機器認証サーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ３００の公開鍵ＫｐＤＡＳを用いて図３３（ｊ）に示す暗号化コンテンツ鍵データ（ＤＡＳ）の電子署名の検証を実行する。なお、先に説明した図３４（ｊ’）の簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）をショップサーバ１００が受領した場合も同様の検証を実行する。さらに、必要に応じて図３３（ｊ）の暗号化コンテンツデータ（ＤＡＳ）内の暗号化コンテンツ鍵１（ショップ１）を検証するようにしてもよい。

【０１８７】（１３）相互認証、および

（１４）暗号化コンテンツ鍵要求データ送信

次に、ユーザ機器２００は、暗号化コンテンツ鍵要求データをショップサーバに対して送信する。なお、この際、前の要求と異なるセッションで要求を実行する場合は、再度相互認証を実行して、相互認証が成立したことを条件として暗号化コンテンツ鍵要求データがユーザ機器２００からショップサーバ１００に送信される。

【０１８８】（１５）検証処理、および

（１６）課金処理

暗号化コンテンツ鍵要求データをユーザ機器から受信したショップサーバ１００は、暗号化コンテンツ鍵要求データの検証処理を実行する。これは、図１５を用いて説明したと同様の処理である。データ検証が済むと、ショップサーバ１００は、コンテンツの取り引きに関する課金処理を実行する。課金処理は、ユーザの取り引き口座からコンテンツ料金を受領する処理である。受領したコンテンツ料金は、コンテンツの著作権者、ショップ、ユーザ機器認証サーバ管理者など、様々な関係者に配分される。

【０１８９】前述した基本モデル１と同様、この課金処理に至るまでには、ユーザ機器認証サーバ３００による暗号化コンテンツ鍵の鍵かけかえ処理プロセスが必須となっているので、ショップサーバ１００は、ユーザ機器間とのみの処理では課金処理が実行できない。また、ユーザ機器２００においても暗号化コンテンツ鍵の復号ができないので、コンテンツの利用ができない。ユーザ機器認証サーバは、図６を用いて説明したユーザ機器認証サーバ・ライセンス管理データベースに、すべての鍵か

けかえ処理を実行したコンテンツ取り引き内容を記録しており、すべての課金対象となるコンテンツ取り引きが把握可能となる。従って、ショップ側単独でのコンテンツ取り引きは不可能となり、不正なコンテンツ販売が防止される。

【０１９０】（１７）暗号化コンテンツ鍵データ２（ショップ）送信

ショップサーバ１００における課金処理が終了すると、ショップサーバ１００は、暗号化コンテンツ鍵データ２（ショップ）をユーザ機器２００に送信する。

【０１９１】暗号化コンテンツ鍵データ２（ショップ）の構成を図３３（ｋ）に示す。暗号化コンテンツ鍵データ２（ショップ）は、暗号化コンテンツ鍵要求の要求元であるユーザ機器２００の識別子であるユーザ機器ＩＤ、ユーザ機器認証サーバ３００から受領した暗号化コンテンツ鍵データ（ＤＡＳ）（図３３（ｊ）のユーザ機器認証サーバ公開鍵証明書を除いたデータ）、を有し、これらのデータに対するショップサーバ１００の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ２（ショップ）には、ショップサーバ１００の公開鍵証明書と、ユーザ機器認証サーバ３００の公開鍵証明書が添付され、ユーザ機器２００に送付される。なお、ユーザ機器２００がユーザ機器認証サーバ公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【０１９２】なお、ユーザ機器認証サーバ３００が信頼できる第三者機関であると認められる存在であり、ショップサーバ１００がユーザ機器認証サーバ３００から受信する暗号化コンテンツ鍵データ（ＤＡＳ）が先に説明した図３４（ｊ’）の簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）である場合は、ショップサーバ１００は、図３４（ｋ’）に示す暗号化コンテンツ鍵データ２（ショップ）をユーザ機器に送付する。すなわち、図３４（ｊ’）に示す簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）にショップサーバの署名を付加したデータに、ショップサーバ１００の公開鍵証明書と、ユーザ機器認証サーバ３００の公開鍵証明書を添付してユーザ機器２００に送付する。

【０１９３】（１８）受信データ検証

ショップサーバ１００から、暗号化コンテンツ鍵データ２（ショップ）を受領したユーザ機器２００は、暗号化コンテンツ鍵データ２（ショップ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器２００は、まずショップサーバ１００から受領したショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバ１００の公開鍵ＫｐＳＨＯＰを用いて図３３（ｋ）に示す暗号化コンテンツ鍵データ２（ショップ）の電子署名の検証を実行する。さらに、ユーザ機器認証サーバ３００の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ３００の公開鍵ＫｐＤＡＳを用いて図３３（ｊ）に示す暗号化コンテンツ鍵データ２（ショップ）に含まれる（１１）暗号化コンテンツ鍵データ（ＤＡＳ）の署名検証を実行する。さらに、必要に応じて図３３（ｊ）の暗号化コンテンツデータ（ＤＡＳ）内の暗号化コンテンツ鍵１（ショップ１）を検証するようにしてもよい。

【０１９４】（１９）保存処理

ショップサーバ１００から受信した暗号化コンテンツ鍵データ２（ショップ）を検証したユーザ機器２００は、暗号化コンテンツ鍵データ２（ショップ）に含まれる自己の公開鍵ＫｐＤＥＶで暗号化された暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を自己の秘密鍵ＫｓＤＥＶを用いて復号し、さらに、ユーザ機器の保存鍵Ｋｓｔｏを用いて暗号化して暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を生成して、これをユーザ機器２００の記憶手段に格納する。コンテンツの利用時には、暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を保存鍵Ｋｓｔｏを用いて復号してコンテンツ鍵Ｋｃを取り出して、取り出したコンテンツ鍵Ｋｃを用いて、暗号化コンテンツＫｃ（Content）の復号処理を実行し、コンテンツ（Content）を再生、実行する。

【０１９５】このように、基本配信モデル２においては、ユーザ機器２００と、ユーザ機器認証サーバ３００との間ではデータの送受信が実行されず、ユーザ機器２００は、ショップサーバ１００との間でデータ送受信を行なうのみでよく、ユーザ機器の処理負担が軽減される。

【０１９６】［１．２．基本コンテンツ配信モデル２の変形例］次に、図３１に示した基本コンテンツ配信モデル２の構成の変形例について説明する。図３５に示す構成は、ショップサーバの機能を分離し、ショップサーバと配信サーバを設けた構成である。ショップサーバ１００は、ユーザ機器２００からのコンテンツ購入要求を受領するが、ユーザ機器２００に対するコンテンツ配信は配信サーバ４００が実行する。本構成では、データ送受信を実行するエンティティ間での相互認証を行なわず、各エンティティは、受信データの署名検証のみを行なう。しかし、基本コンテンツ配信モデル２同様、エンティティ間で相互認証処理を行なう構成をとっても構わない。

【０１９７】ショップサーバ１００は、ユーザ機器２００からの購入要求データを受信し、データの検証（図３５の処理（３））を行なって、要求データの正当性を確認した後、配信サーバ４００に対して、コンテンツ配信要求の送信を実行（図３５の処理（４））する。配信サーバ４００は、ショップサーバ１００からのコンテンツ配信要求データを検証し、データの正当性が確認された

場合、コンテンツデータベース４１０から取り出した暗号化コンテンツを送信（図３５の処理（６））する。

【０１９８】ユーザ機器２００は、配信サーバ４００から、暗号化コンテンツを受信し、データ検証の後、暗号化コンテンツ受領データを配信サーバ４００に送信（図３５の処理（８））する。配信サーバ４００は、受信データ検証の後、ユーザ機器認証サーバ３００に対して暗号化コンテンツ鍵データ（配信サーバ）および暗号化コンテンツ鍵かけかえ要求を送信（図３５の処理（１０））する。

【０１９９】ユーザ機器認証サーバ３００が配信サーバ４００から暗号化コンテンツ鍵データ（配信サーバ）および暗号化コンテンツ鍵かけかえ要求を受信した以後の処理は、相互認証処理を省略した以外は、先の図３１に示した構成に基づく実施例と同様となる。

【０２００】本構成においては、ユーザ機器は、相互認証を行なわずに、ショップサーバに対してコンテンツ購入要求を送信し、配信サーバから暗号化コンテンツを受領する。ショップサーバ１００は、ユーザ機器からのコンテンツ要求を受け付けて、その正当性を署名検証のみに基づいて検証する。さらに、ユーザ機器認証サーバからの、かけかえ済みの暗号化コンテンツ鍵を受信し、その正当性を署名検証により実行する。配信サーバ４００は、ショップサーバからの受信データについての署名検証を実行してデータ正当性の確認を行ないコンテンツ配信を行なう。

【０２０１】ショップサーバ１００は、コンテンツ自体の管理、配信を行なわない。従って、例えば音楽データを管理する音楽コンテンツ配信サーバ、ゲームコンテンツを管理するゲームコンテンツ配信サーバ等、様々なコンテンツ管理主体となる複数の配信サーバに対して１つのショップサーバがユーザ機器からのコンテンツ要求に応答し、ショップサーバが要求に応じて要求コンテンツを管理する配信サーバにコンテンツ配信要求を送信する構成に適した態様である。また、この構成にしたことにより、例えば、ユーザ機器とショップサーバは双方向通信であるため、インターネットを使うが、配信サーバからユーザ機器へは片方向通信であるため、高速な衛星通信が利用できるメリットがある。

【０２０２】本実施例では、相互認証が省略され、署名検証のみにより、データの正当性を確認する処理としたので、処理の効率化が実現される。

【０２０３】図３６は、図３５と同様ショップサーバの機能を分離し、ショップサーバと配信サーバを設け、相互認証を省略した構成であり、ショップサーバ１００は、ユーザ機器２００からのコンテンツ購入要求を受領し、署名検証を行なう。ユーザ機器２００に対するコンテンツ配信は配信サーバ４００が実行する。図３５の構成と異なる点は、ショップサーバ１００から配信サーバ４００に対してコンテンツ配信要求を送信せず、ユーザ機器認証サーバ３００が、配信サーバ４００に対してコンテンツ配信要求を送信する構成とした点である。

【０２０４】ショップサーバ１００は、ユーザ機器２００からの購入要求データを受信し、データの検証（図３６の処理（３））を行なって、要求データの正当性を確認した後、ユーザ機器認証サーバ３００に対して、暗号化コンテンツ鍵データ１（ショップ）の送信を実行（図３６の処理（４））する。その後、ユーザ機器認証サーバ３００は、データの検証（図３６の処理（５））を行なって、要求データの正当性を確認した後、配信サーバ４００に対して、コンテンツ配信要求の送信を実行（図３６の処理（６））する。配信サーバ４００は、ユーザ機器認証サーバ３００からのコンテンツ配信要求データを検証し、正当性が確認された場合、ユーザ機器２００に対して、コンテンツデータベース４１０から取り出した暗号化コンテンツを送信（図３６の処理（８））する。以後の処理は、先の図３５に示した構成に基づく処理と同様となる。

【０２０５】本構成においては、ユーザ機器認証サーバ３００は、配信サーバ４００からの鍵のかけかえ要求以前、ショップサーバ１００に対してコンテンツ購入要求があった時点で、コンテンツ購入要求主体であるユーザ機器情報を取得し、管理することが可能となる。従って、配信サーバ４００からの鍵のかけかえ要求受領時に、すでに登録済みのコンテンツ購入要求ユーザ機器であるか否かの照合処理が可能となる。また、ＤＡＳが信頼できる機関であるとみなせば、配信サーバはショップサーバの送信データを検証しなくてもよくなり、処理の効率化が図れる。

【０２０６】以上、説明したように、本発明のコンテンツ配信構成によれば、ユーザ機器は、暗号化コンテンツＫｃ（Content）取得後、コンテンツ利用可能な状態に至るまでには、ユーザ機器認証サーバにおける暗号化コンテンツ鍵の鍵かけかえ処理プロセスが必須となる。従って、ショップサーバが、ユーザ機器に対して、ユーザ機器認証サーバに通知せずコンテンツを販売し、コンテンツをユーザ機器において利用可能な状態とすることができない。ユーザ機器認証サーバは、ユーザ機器認証サーバ・ライセンス管理データベース（図６参照）に、すべての鍵かけかえ処理を実行したコンテンツ取り引き内容を記録しており、すべてのショップの取り引きの管理が可能であり、課金されたコンテンツ取り引きを把握し、ショップの課金処理において受領されたコンテンツ料金を、コンテンツの著作権者、ショップ、ユーザ機器認証サーバ管理者など、様々な関係者に正確に配分することが可能となり、不正なコンテンツ利用を排除する構成が実現される。

【０２０７】［２．電子チケットを利用したコンテンツ配信モデル］次に、ユーザによるコンテンツの利用（購入）に基づいて、コンテンツの著作権者、製作者、ライ

センスホルダー、ショップ等、様々な関係者に対する利益配分情報を記述した電子チケットを発行して、発行した電子チケットに基づく利益配分処理を実行する構成について説明する。

【０２０８】図３７に電子チケットに基づく利益配分を実行するシステム構成を示す。図３７のコンテンツ配信システムは、ユーザ機器が購入するコンテンツの購入要求を受け付け、コンテンツ購入に伴う利用料金の利益配分情報を記述した電子チケットを発行するチケット発行サーバ（ＴＩＳ：Ticket Issuer Server）６１０、コンテンツ購入主体となるユーザ機器（ＤＥＶ）６２０、正当なコンテンツ取り引き管理のための鍵かけかえ処理を行なう管理サーバとして機能するユーザ機器認証サーバ（ＤＡＳ：Device Authentication Server）６３０、コンテンツの配信を行なうコンテンツプロバイダ（ＣＰ）等の配信サーバ（ＣＰ：Content Provider）６４０、さらに、電子チケットに基づいて利用料金の振替等の換金処理を行なうチケット換金サーバ（ＴＥＳ：Ticket Exchange Server）６５０を主構成要素とする。

【０２０９】（チケット発行サーバ）図３７のコンテンツ配信システムのチケット発行サーバ（ＴＩＳ）６１０の構成を図３８に示す。チケット発行サーバ６１０は、ユーザ機器６２０からの購入要求を受け付け、購入要求のあった取り引き対象となるコンテンツに対応してその利益配分情報を記述した電子チケットを発行する。

【０２１０】チケット発行サーバ（ＴＩＳ）６１０は、コンテンツ取り引きに伴う発行チケットの管理データ、例えばコンテンツ販売先のユーザ機器の識別子とコンテンツ識別子、コンテンツ料金等を対応づけて管理するチケット発行管理データベース６１２を有する。さらに、ユーザ機器６２０からのコンテンツ購入要求検証、チケット発行管理データベースの制御、チケットに基づくユーザ機器に対する課金処理、ユーザ機器等との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段６１３を有する。

【０２１１】チケット発行管理データベース６１２のデータ構成を図３９に示す。チケット発行管理データベース６１２は、チケット発行サーバがコンテンツ取り引きに応じてチケット発行処理を実行する際に内部生成する識別番号としてのチケット発行処理Ｎｏ．、コンテンツ購入依頼を発行したユーザ機器の識別子である機器ＩＤ、ユーザ機器とチケット発行サーバ間での取り引きを実行する際に、コンテンツ取り引き識別子としてユーザ機器で生成発行するトランザクションＩＤ、取り引き対象コンテンツの識別子であるコンテンツＩＤ、チケット発行サーバ６１０の発行する電子チケットに基づいて対価を得るエンティテイ、例えば著作権者、ライセンスホルダ、管理者、コンテンツ販売関係者等の識別子としてのチケット利用先ＩＤ、各チケット利用先ＩＤに対応するコンテンツ利用料金配分金額としての金額、チケットに基づく換金処理の有効期限、チケット発行サーバ６１０におけるチケット発行、管理処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【０２１２】チケット発行サーバ６１０の制御手段６１３は、図３８に示すように暗号処理手段、通信処理手段としての機能も有し、制御手段６１３は、例えば暗号処理プログラム、通信処理プログラムを格納したコンピュータによって構成される。制御手段６１３の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。チケット発行サーバ６１０が格納する暗号鍵等の暗号処理用データとしては、チケット発行サーバ６１０の秘密鍵：ＫｓＴＩＳ、チケット発行サーバ６１０の公開鍵証明書Ｃｅｒｔ＿ＴＩＳ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡがある。

【０２１３】制御手段６１３の構成は、先に図４を用いて説明した制御手段構成と同様の構成、すなわち、中央演算処理装置（ＣＰＵ:Central Processing Unit）、ＲＯＭ（Read only Memory）、ＲＡＭ（Random Access Memory）、表示部、入力部、記憶手段、通信インタフェース等を持つ構成である。

【０２１４】（ユーザ機器）ユーザ機器（ＤＥＶ）６２０は、図１の構成におけるユーザ機器、すなわち、図７の構成と同様の構成を持つ。ユーザ機器６２０が格納する暗号鍵等の暗号処理用データとしては、ユーザ機器の秘密鍵：ＫｓＤＥＶ、ユーザ機器の公開鍵証明書Ｃｅｒｔ＿ＤＥＶ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡ、コンテンツをユーザ機器の例えばハードディスク等の記憶手段に格納する際の暗号化鍵として適用する保存鍵Ｋｓｔｏがある。

【０２１５】図３７のチケット管理構成を実行するシステムにおけるユーザ機器６２０の有する購入管理データベースは、チケット管理機能を持つデータ構成となる。購入管理データベースのデータ構成を図４０に示す。購入管理データベースは、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するトランザクションＩＤ、取り引き対象コンテンツの識別子であるコンテンツＩＤ、コンテンツ取り引きに伴いチケットを発行するチケット発行体の識別子であるチケット発行体ＩＤ、チケット発行サーバ６１０が設定するチケット発行処理Ｎｏ．、チケットを送信した先の送信先エンティテイの識別子としてのチケット送信先ＩＤ、さらに、ユーザ機器におけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【０２１６】（ユーザ機器認証サーバ）ユーザ機器認証サーバ（ＤＡＳ）６３０は、図１の構成におけるユーザ機器認証サーバ、すなわち、図５の構成と同様の構成を持つ。ユーザ機器認証サーバ６３０が格納する暗号鍵等の暗号処理用データとしては、ユーザ機器認証サーバ（ＤＡＳ）の秘密鍵：ＫｓＤＡＳ、ユーザ機器認証サーバ（ＤＡＳ）の公開鍵証明書Ｃｅｒｔ＿ＤＡＳ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡがある。

【０２１７】図３７のチケット管理構成を実行するシステムにおけるユーザ機器認証サーバ６３０の有するライセンス管理データベースは、チケット管理機能を持つデータ構成となる。ライセンス管理データベースのデータ構成を図４１に示す。ライセンス管理データベースは、コンテンツ取り引き時にユーザ機器認証サーバ（ＤＡＳ）６３０の実行する処理に応じて内部生成する処理識別子としてのユーザ機器認証サーバ処理Ｎｏ．、コンテンツ購入依頼を発行したユーザ機器の識別子である機器ＩＤ、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するトランザクションＩＤ、取り引き対象コンテンツの識別子であるコンテンツＩＤ、コンテンツ取り引きに伴いチケットを発行するチケット発行体の識別子であるチケット発行体ＩＤ、チケット発行サーバ６１０が設定するチケット発行処理Ｎｏ．、さらに、ユーザ機器認証サーバ（ＤＡＳ）におけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【０２１８】（配信サーバ）図３７のコンテンツ配信システムの配信サーバ６４０の構成を図４２に示す。配信サーバ６４０は、例えばコンテンツプロバイダ（ＣＰ）であり、取り引き対象となるコンテンツをコンテンツキーで暗号化した暗号化コンテンツデータであるＫｃ（Ｃｏｎｔｅｎｔ）と、コンテンツキーＫｃをユーザ機器認証サーバ（ＤＡＳ：Device Authentication Server）の公開鍵：ＫｐＤＡＳで暗号化した暗号化コンテンツキーＫｐＤＡＳ（Ｋｃ）を格納したコンテンツデータベース６４４を有する。なお、暗号化コンテンツデータであるＫｃ（Ｃｏｎｔｅｎｔ）は、図にも示すように、それぞれコンテンツ識別子であるコンテンツＩＤが付加され、コンテンツＩＤに基づいて識別可能な構成を持つ。

【０２１９】配信サーバ６４０は、さらにコンテンツの配信管理データを管理する配信管理データベース６４２を有する。配信管理データベース６４２は、チケット管理機能を持つデータ構成となる。購入管理データベースのデータ構成を図４３に示す。配信管理データベース６４２は、コンテンツ配信処理を実行する際に、配信サーバ６４０が設定する配信サーバ処理Ｎｏ．、取り引き対象コンテンツの識別子であるコンテンツＩＤ、コンテンツの配信対象識別子としてのユーザ機器ＩＤ、コンテンツ取り引きに伴いチケットを発行するチケット発行体の識別子であるチケット発行体ＩＤ、チケット発行体が設定するチケット発行処理Ｎｏ．、さらに、配信サーバにおけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される

【０２２０】さらに、配信サーバ６４０は、コンテンツデータベース６４４からの配信コンテンツの抽出処理、取り引きに伴う配信管理データベース６４２に対して登録する取り引きデータの生成処理、ユーザ機器６２０他との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段６４３を有する。制御手段６４３は、図４２に示すように暗号処理手段、通信処理手段としての機能も有し、制御手段６４３は、例えば暗号処理プログラム、通信処理プログラムを格納したコンピュータによって構成される。制御手段６４３の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。配信サーバ６４０が格納する暗号鍵等の暗号処理用データとしては、配信サーバ６４０の秘密鍵：ＫｓＣＰ、配信サーバ６４０の公開鍵証明書Ｃｅｒｔ＿ＣＰ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡがある。

【０２２１】制御手段６４３の構成は、先に図４を用いて説明した制御手段構成と同様の構成、すなわち、中央演算処理装置（ＣＰＵ:Central Processing Unit）、ＲＯＭ（Read only Memory）、ＲＡＭ（Random Access Memory）、表示部、入力部、記憶手段、通信インタフェース等を持つ構成である。

【０２２２】（チケット換金サーバ）図３７のコンテンツ配信システムのチケット換金サーバ（ＴＥＳ）６５０の構成を図４４に示す。チケット換金サーバ６５０は、様々なエンティティから電子チケットを受信し、受信データの検証の後、チケットに基づく換金処理、例えば口座振替処理、あるいは電子マネーの残高変更処理等を行なう、具体的な一例としては、チケット換金サーバ６５０は各エンティティの銀行口座を管理する銀行内のサーバとする設定が可能である。

【０２２３】チケット換金サーバ６５０は、コンテンツ取り引きに伴う発行チケットに基づく換金処理の管理データを管理するチケット換金管理データベース６５２を有する。さらに、各エンティティからの受信チケット検証、チケット換金管理データベースの制御、各エンティティとの通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段６５３を有する。

【０２２４】チケット換金管理データベース６５２のデータ構成を図４５に示す。チケット換金管理データベー

ス６５２は、チケット換金サーバが受領チケットに応じてチケット換金処理を実行する際に内部生成する識別番号としてのチケット換金サーバ処理Ｎｏ．、チケットに基づく換金の要求を行なってきた要求主体識別子としての換金依頼元ＩＤ、コンテンツ取り引きに伴いチケットを発行するチケット発行体の識別子であるチケット発行体ＩＤ、チケット発行サーバ６１０が設定するチケット発行処理Ｎｏ．、チケットに基づく換金金額、コンテンツの購入主体であるユーザ機器の識別子としてのユーザ機器ＩＤ、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するトランザクションＩＤ、さらに、チケット換金サーバにおける換金処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【０２２５】さらに、チケット換金サーバ６５０は、チケット換金管理データベース６５２のデータ生成、更新処理、受領チケットの検証処理、各種エンティテイとの通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段６５３を有する。制御手段６５３は、図４４に示すように暗号処理手段、通信処理手段としての機能も有し、制御手段６５３は、例えば暗号処理プログラム、通信処理プログラムを格納したコンピュータによって構成される。制御手段６５３の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。チケット換金サーバ６５０が格納する暗号鍵等の暗号処理用データとしては、チケット換金サーバ６５０の秘密鍵：ＫｓＴＥＳ、チケット換金サーバ６５０の公開鍵証明書Ｃｅｒｔ＿ＴＥＳ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡがある。

【０２２６】制御手段６５３の構成は、先に図４を用いて説明した制御手段構成と同様の構成、すなわち、中央演算処理装置（ＣＰＵ:Central Processing Unit）、ＲＯＭ（Read only Memory）、ＲＡＭ（Random Access Memory）、表示部、入力部、記憶手段、通信インタフェース等を持つ構成である。

【０２２７】［コンテンツ購入処理］次に、図３７に戻り、ユーザ機器が、チケット発行サーバにコンテンツ購入要求を発行してコンテンツを利用可能な状態としてユーザ機器に保存し、チケットに基づいてコンテンツ料金が配分（換金）されるまでの処理について説明する。図３７の番号（１）から（３２）の順に処理が進行する。各番号順に処理の詳細を説明する。

【０２２８】（１）相互認証

コンテンツを購入しようとするユーザ機器６２０は、チケット発行サーバ６１０との間で相互認証処理を行なう。相互認証処理は、図１２または図１３を用いて説明した処理である。相互認証処理において、生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。

【０２２９】（２）トランザクションＩＤ、購入要求データ生成、および

（３）購入要求データ送信

チケット発行サーバ６１０とユーザ機器６２０間の相互認証が成功すると、ユーザ機器６２０は、コンテンツの購入要求データを生成する。購入要求データの構成を図４６（ｍ）に示す。購入要求データは、コンテンツ購入の要求元であるユーザ機器６２０の識別子である機器ＩＤ、取り引きの識別子として、ユーザ機器６２０の暗号処理手段が例えば乱数に基づいて生成するトランザクションＩＤ、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツＩＤの各データを有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、購入要求データには、署名検証用に必要に応じてユーザ機器の公開鍵証明書を添付する。

【０２３０】（４）受信データ検証

図４６（ｍ）に示す購入要求データをユーザ機器６２０から受信したチケット発行サーバ６１０は、受信データの検証処理を実行する。検証処理の詳細は、先に図１５を用いて説明した通りである。

【０２３１】（５）課金処理

（６）電子チケット発行

（７）電子チケット送信

チケット発行サーバ６１０は、次に、コンテンツの取り引きに関する課金処理、電子チケット発行処理を実行する。これらの処理は、例えば予め登録されているユーザ口座、あるいは電子マネー口座等に基づいて設定されるユーザの取り引き金額限度内の電子チケットを発行する処理として実行される。発行された電子チケットは、ユーザ機器６２０に送信される。

【０２３２】電子チケットの構成例を図４７に示す。図４７（Ａ）は、電子チケットに基づく料金配分先（料金受領エンティテイ）が単一である場合のデータ構成であり、チケット発行体ＩＤ、チケット発行処理Ｎｏ．、電子チケットに基づく料金配分先（エンティテイ）を示すチケット利用先ＩＤ、電子チケットに基づいて配分される料金を示す金額、電子チケットの有効期限、すなわち料金受領エンティテイがチケットに基づく換金（料金精算）処理を実行可能な期限、さらに、ユーザ機器からチケット発行サーバに対して送信された購入要求データ（図４６（ｍ）参照）を含む。なお、さらに、チケット発行日等のデータを付加してもよい。これらのデータにチケット発行サーバ６１０の電子署名が付加される。さらに、電子チケットには、署名検証用に必要に応じてチケット発行サーバの公開鍵証明書を添付する。

【０２３３】図４７（Ｂ）は、電子チケットに基づく料金配分先（エンティテイ）が複数である場合のデータ構

成であり、チケット利用先ＩＤが複数（１～ｎ）格納され、それぞれのチケット利用先ＩＤ毎に、電子チケットに基づいて配分される料金を示す金額が１～ｎまで格納されている。チケットに基づいて料金を受領するエンティテイは、自己のＩＤに対応する金額を受領する。

【０２３４】図３７の処理例では、チケット発行サーバ６１０は、配信サーバを管理するコンテンツプロバイダ（ＣＰ）用の電子チケットと、ユーザ機器認証サーバ（ＤＡＳ）用の電子チケットを発行する。これらのチケット発行先は、コンテンツ毎に異なり、コンテンツの著作者等が含まれる場合もある。チケット発行サーバは、コンテンツＩＤに基づいてチケット発行先と、配分金額を定めたテーブルを有し、ユーザ機器からのコンテンツ購入要求に含まれるコンテンツＩＤに基づいてテーブルからチケット発行先と、配分金額データを取得してチケットを生成して発行する。

【０２３５】（８）受信データ検証

チケット発行サーバ６１０からチケットを受信したユーザ機器６２０は、チケットの検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器６２０は、まずチケット発行サーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したチケット発行サーバの公開鍵ＫｐＴＩＳを用いてチケットの署名検証を実行する。

【０２３６】（９）相互認証

（１０）電子チケット（ＣＰ用）送信

次にユーザ機器６２０は、配信サーバ６４０にアクセスし、相互認証処理を実行する。相互認証が成立すると、ユーザ機器６２０は、配信サーバ６４０に対して、配信サーバ用の電子チケット（ＣＰ用）を送信する。

【０２３７】（１１）受信データ検証

（１２）暗号化コンテンツおよび暗号化コンテンツ鍵送信

配信サーバ６４０において、電子チケット（ＣＰ用）の検証が完了し、データ改竄のない正当な電子チケットであると判定すると、配信サーバ６４０は、暗号化コンテンツおよび暗号化コンテンツ鍵をユーザ機器に送信する。これらは、コンテンツをコンテンツキーで暗号化した暗号化コンテンツ：Ｋｃ（content）と、コンテンツキー：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）６３０の公開鍵で暗号化した暗号化コンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）を含むデータである。

【０２３８】（１３）受信データ検証

（１４）相互認証

（１５）電子チケット（ＤＡＳ用）および鍵かけかえ要求送信

配信サーバ６４０から暗号化コンテンツおよび暗号化コンテンツ鍵を受信したユーザ機器６２０は、データの検証処理を実行する。データ検証後、ユーザ機器６２０は、ユーザ機器認証サーバ６３０にアクセスし、相互認証処理を実行する。相互認証が成立すると、ユーザ機器６２０は、ユーザ機器認証サーバ６３０に対して、ユーザ機器認証サーバ用の電子チケット（ＤＡＳ）および鍵かけかえ要求を送信する。鍵かけかえ要求は、先に配信サーバ６４０から受信したユーザ機器認証サーバの公開鍵で暗号化されたコンテンツ鍵Ｋｃである。暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）をユーザ機器の公開鍵ＫｐＤＥＶで暗号化したコンテンツ鍵、すなわちＫｐＤＥＶ（Ｋｃ）とする処理を要求するものであり、図１を用いて説明したかけかえ処理と同様である。

【０２３９】（１６）受信データ検証

（１７）暗号化コンテンツ鍵かけかえ処理、ユーザ機器６２０から電子チケット（ＤＡＳ用）および暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）かけかえ要求を受信したユーザ機器認証サーバ６３０は、電子チケット（ＤＡＳ用）、暗号化コンテンツ鍵かけかえ要求の検証処理を実行する。検証が終了し、データの改竄のない正当な電子チケットであり、正当な鍵かけかえ要求であると判定すると、ユーザ機器認証サーバ６３０は、コンテンツ鍵：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）６３０の公開鍵ＫｐＤＡＳで暗号化したデータ：ＫｐＤＡＳ（Ｋｃ）をユーザ機器認証サーバ６３０の秘密鍵ＫｓＤＡＳで復号してコンテンツ鍵Ｋｃを取得し、さらにコンテンツ鍵Ｋｃをユーザ機器の公開鍵：ＫｐＤＥＶで暗号化した暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を生成する。すなわち、ＫｐＤＡＳ（Ｋｃ）→Ｋｃ→ＫｐＤＥＶ（Ｋｃ）の鍵かけかえ処理を実行する。この処理は、前述の図１６を用いて説明した処理と同様である。

【０２４０】（１８）暗号化コンテンツ鍵送信

（１９）受信データ検証

（２０）保存処理

ユーザ機器認証サーバ６３０は、鍵かけかえにより生成した暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）をユーザ機器６２０に送信する。ユーザ機器認証サーバ６３０から、暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）を受領したユーザ機器６２０は、受信データ検証処理を実行し、検証後、ユーザ機器６２０は、暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）を自己の秘密鍵ＫｓＤＥＶを用いて復号し、さらに、ユーザ機器の保存鍵Ｋｓｔｏを用いて暗号化して暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を生成して、これをユーザ機器６２０の記憶手段に格納する。コンテンツの利用時には、暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を保存鍵Ｋｓｔｏを用いて復号してコンテンツ鍵Ｋｃを取り出して、取り出したコンテンツ鍵Ｋｃを用いて、暗号化コンテンツＫｃ（Content）の復号処理を実行し、コンテンツ（Content）を再生、実行する。

【０２４１】（２１）相互認証

（２２）電子チケット（ＣＰ用）送信

配信サーバ６４０は、ユーザ機器６２０に対する暗号化

コンテンツ配信の後、チケット換金サーバ６５０にアクセスし、相互認証処理を実行する。相互認証が成立すると、配信サーバ６４０は、チケット換金サーバ６５０に対して、配信サーバ用の電子チケット（ＣＰ用）を送信する。

【０２４２】（２３）受信データ検証、換金処理

チケット換金サーバ６５０において、電子チケット（ＣＰ用）の検証が完了し、データ改竄のない正当な電子チケットであると判定すると、チケット換金サーバ６５０は、受領した電子チケット（ＣＰ用）に基づいて換金処理を実行する。換金処理は、例えば予め登録されている配信サーバを管理するコンテンツプロバイダ（ＣＰ）の管理口座、あるいは電子マネー口座等に、電子チケット（ＣＰ用）に設定された金額をユーザ機器の管理ユーザの口座から振り替える処理として行われる。あるいは既にチケット発行サーバがユーザからの前払い預り金として受領しているチケット発行サーバ管理口座からコンテンツプロバイダ（ＣＰ）の管理口座にチケットに設定された金額を振り替える処理として行なってもよい。なお、チケット換金サーバ６５０は、チケットに格納された有効期限を検証し、有効期限内であることが確認されたことを条件として該チケットに基づく料金精算処理を実行する。

【０２４３】（２４）換金処理レポート報告

チケット換金サーバ６５０において、電子チケット（ＣＰ用）に基づく換金が終了すると、チケット換金サーバ６５０は、配信サーバ６４０に対して換金処理が済んだことを示すレポートを送信する。

【０２４４】換金処理レポートの構成例を図４６（ｎ）に示す。換金処理レポートは、チケット換金処理個々の識別子であるチケット換金処理ＩＤ、チケットに基づく換金の要求を行なってきた要求主体識別子としての換金依頼元ＩＤ、チケットに基づく換金金額、コンテンツ取り引きに伴いチケットを発行したチケット発行体の識別子であるチケット発行体ＩＤ、チケット発行サーバ６１０が設定するチケット発行処理Ｎｏ．、チケット換金サーバ６５０において換金処理が実行されたチケット換金処理完了日等のデータを有し、これらにチケット換金サーバ６５０の電子署名が付加される。さらに、換金処理レポートには、署名検証用に必要に応じてチケット換金サーバの公開鍵証明書を添付する。

【０２４５】（２５）受信データ検証

チケット換金サーバ６５０から換金処理レポートを受信した配信サーバ６４０は、換金処理レポートの検証処理を実行する。データ検証により、レポートが正当であると認められれば、配信サーバの管理主体であるコンテンツプロバイダに対するコンテンツ取り引きに伴う料金配分が完了したことが確認される。

【０２４６】（２６）相互認証

（２７）電子チケット（ＤＡＳ用）送信

（２８）受信データ検証、換金処理

（２９）換金処理レポート報告

（３０）受信データ検証

ユーザ機器認証サーバ６３０とチケット換金サーバ６５０との間においても、上述の配信サーバ６４０とチケット換金サーバ６５０間の処理（２１）～（２５）と同様の処理が電子チケット（ＤＡＳ用）に基づいて実行される。

【０２４７】（３１）相互認証

（３２）換金処理レポート報告

（３３）受信データ検証

また、チケット換金サーバ６５０は、各エンティティから受領したチケットに基づいて換金処理を実行した場合、チケット発行サーバ６１０との相互認証後、各エンティティに送付したと同様の換金処理レポート（図４６（ｎ）参照）をチケット発行サーバ６１０に送信する。チケット発行サーバ６１０は、チケット換金サーバ６５０から受信した換金処理レポートの検証を実行し、発行したチケットに関する換金処理が完了したことを確認する。

【０２４８】（各機器におけるステータス遷移）図３７に示すチケット発行サーバ６１０等の各エンティティは、それぞれコンテンツ取り引きに係る一連の処理において、処理状態を示すステータスに応じて、次の処理を決定する。ステータスは、例えば図３９に示すチケット発行管理データベース、図４０のユーザ機器の購入管理データベース等において、各コンテンツ取り引き毎に管理される。

【０２４９】まず、チケット発行サーバ６１０のステータス遷移について、図４８を用いて説明する。チケット発行サーバ６１０は、ユーザ機器６２０からのコンテンツ購入要求データを受信（図３７の処理（３）に対応）することで処理が開始される。チケット発行サーバ６１０は、ユーザ機器６２０からの受信データを検証し、検証に成功した場合は、ステータスを「購入受付完了」に設定し、データ検証により正当な購入要求であるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、購入受付処理を所定回数繰り返した後処理を中止し、ステータスを「購入受付失敗」とする。ステータスが「購入受付完了」である場合にのみ次ステップに進む。

【０２５０】ステータスが「購入受付完了」に遷移すると、次に、チケット発行サーバ６１０は、ユーザ機器６２０に対して電子チケットを送信（図３７の処理（７）に対応）し、ユーザ機器からの受信応答（レスポンス）を受領することにより、ステータスを「チケット配信完了」とする。受信応答（レスポンス）を受領しなかった場合は、処理を中止するか、あるいは同様の処理、ここでは、電子チケットの送信処理を所定回数繰り返した後、処理を中止し、ステータスを「チケット配信失敗」

とする。ステータスが「チケット配信完了」である場合にのみ次ステップに進む。

【０２５１】ステータスが「チケット配信完了」に遷移した場合、次に、チケット発行サーバ６１０は、チケット換金サーバから換金処理レポートを受信し、レポートの検証（図３７の処理（３２）、（３３）に対応）を実行する。検証に成功した場合は、ステータスを「換金処理レポート受信完了」に設定し、処理終了とする。レポート検証により正当なレポートであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、レポート受信、検証処理を所定回数繰り返した後、処理を中止し、ステータスを「換金レポート受信失敗」とする。チケット発行サーバ６１０は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【０２５２】次にユーザ機器認証サーバ６３０のステータス遷移について、図４９を用いて説明する。ユーザ機器認証サーバ６３０は、ユーザ機器６２０からの暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を受信（図３７の処理（１５）に対応）することで処理が開始される。ユーザ機器認証サーバ６３０は、ユーザ機器６２０からの電子チケット（ＤＡＳ）を含む受信データを検証し、検証に成功した場合は、ステータスを「鍵受信完了」に設定し、データ検証により正当なデータであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵データ（ユーザ機器）の受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵受信失敗」とする。ステータスが「鍵受信完了」である場合にのみ次ステップに進む。

【０２５３】ステータスが「鍵受信完了」に遷移すると、次に、ユーザ機器認証サーバ６３０は、コンテンツ鍵かけかえ処理（図３７の処理（１７）に対応）を実行し、鍵かけかえ処理が成功した場合には、ステータスを「鍵かけかえ完了」とする。鍵かけかえに失敗することは想定していないので、ここでは「鍵かけかえ完了」のみのステータス遷移が存在する。

【０２５４】ステータスが「鍵かけかえ完了」に遷移した場合、次に、ユーザ機器認証サーバ６３０は、ユーザ機器６２０に対して暗号化コンテンツ鍵データ（ＤＡＳ）を送信（図３７の処理（１８）に対応）し、ユーザ機器６２０からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「鍵送信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵データ（ＤＡＳ）の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵送信失敗」とする。

【０２５５】ステータスが「鍵送信完了」に遷移すると、次に、ユーザ機器認証サーバ６３０は、チケット換金サーバ６５０に対して、電子チケット（ＤＡＳ用）を送信（図３７の処理（２７）に対応）し、チケット換金サーバ６５０からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「チケット換金要求送信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、チケット換金要求の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「チケット換金要求失敗」とする。

【０２５６】ステータスが「チケット換金要求送信完了」に遷移すると、次に、ユーザ機器認証サーバ６３０は、チケット換金サーバ６５０からの換金処理レポートを受信し、レポートの検証処理（図３７の処理（２９）、（３０）に対応）を実行する。検証に成功した場合は、ステータスを「換金処理レポート受信完了」に設定し、処理終了とする。レポート検証により正当なレポートであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、レポート受信、検証処理を所定回数繰り返した後、処理を中止し、ステータスを「換金レポート受信失敗」とする。ユーザ機器認証サーバ６３０は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【０２５７】次に配信サーバ６４０のステータス遷移について、図５０を用いて説明する。配信サーバ６４０は、ユーザ機器６２０からの電子チケット（ＣＰ用）を受信（図３７の処理（１０）に対応）することで処理が開始される。配信サーバ６４０は、ユーザ機器６２０からの受信データを検証し、検証に成功した場合は、ステータスを「電子チケット受信完了」に設定し、データ検証により正当なデータであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、チケットの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「電子チケット受信失敗」とする。ステータスが「電子チケット受信完了」である場合にのみ次ステップに進む。

【０２５８】ステータスが「電子チケット受信完了」に遷移すると、次に、配信サーバ６４０は、ユーザ機器６２０に対して暗号化コンテンツおよび暗号化コンテンツ鍵データＫｐＤＡＳ（Ｋｃ）を送信（図３７の処理（１２）に対応）し、ユーザ機器６２０からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「配信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツおよび暗号化コンテンツ鍵データＫｐＤＡＳ（Ｋｃ）の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「配信失敗」とする。

【０２５９】ステータスが「配信完了」に遷移すると、次に、配信サーバ６４０は、チケット換金サーバ６５０に対して、電子チケット（ＣＰ用）を送信（図３７の処

理（２２）に対応）し、チケット換金サーバ６５０からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「チケット換金要求送信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、チケット換金要求の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「チケット換金要求失敗」とする。

【０２６０】ステータスが「チケット換金要求送信完了」に遷移すると、次に、配信サーバ６４０は、チケット換金サーバ６５０からの換金処理レポートを受信し、レポートの検証処理（図３７の処理（２４）、（２５）に対応）を実行する。検証に成功した場合は、ステータスを「換金処理レポート受信完了」に設定し、処理終了とする。レポート検証により正当なレポートであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、レポート受信、検証処理を所定回数繰り返した後、処理を中止し、ステータスを「換金レポート受信失敗」とする。配信サーバ６４０は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【０２６１】次に、ユーザ機器６２０のステータス遷移について、図５１を用いて説明する。ユーザ機器６２０は、まず、チケット発行サーバ６１０に対して購入要求データを送信（図３７の処理（３）に対応）することで処理が開始される。ユーザ機器６２０は、チケット発行サーバ６１０に対する購入要求データの受信完了のレスポンスを受信すると、ステータスを「購入要求送信完了」に設定し、チケット発行サーバ６１０からの受信完了のレスポンスを受信できない場合は、処理を中止するか、あるいは同様の処理、ここでは、購入要求送信処理を所定回数繰り返した後、処理を中止し、ステータスを「購入要求送信失敗」とする。ステータスが「購入要求送信完了」である場合にのみ次ステップに進む。

【０２６２】ステータスが「購入要求送信完了」に遷移すると、次に、ユーザ機器６２０は、チケット発行サーバ６１０から、電子チケットを受信（図３７の処理（７）、（８）に対応）し、受信データを検証する。チケット発行サーバ６１０からのチケットの検証に成功した場合は、ステータスを「電子チケット受信完了」に設定し、データ検証により正当なチケットであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、チケット受信処理を所定回数繰り返した後、処理を中止し、ステータスを「電子チケット受信失敗」とする。ステータスが「電子チケット受信完了」である場合にのみ次ステップに進む。

【０２６３】ステータスが「電子チケット受信完了」に遷移した場合、次に、ユーザ機器６２０は、配信サーバ６４０に対して、電子チケットを送信（図３７の処理（１０）に対応）し、データ受信レスポンスを受信する。データ受信レスポンスを受信した場合は、ステータスを「電子チケット送信完了」に設定し、データ受信レスポンスを受信しない場合は、処理を中止するか、あるいは同様の処理、ここでは、チケット送信処理を所定回数繰り返した後、処理を中止し、ステータスを「電子チケット送信失敗」とする。ステータスが「電子チケット送信完了」である場合にのみ次ステップに進む。

【０２６４】ステータスが「電子チケット送信完了」に遷移すると、次に、ユーザ機器６２０は、配信サーバ６４０から、暗号化コンテンツと、暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を受信し、データ検証（図３７の処理（１２）、（１３）に対応）を実行する。データ検証に成功した場合は、ステータスを「鍵１受信完了」に設定し、データ検証に成功しなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵データの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵１受信失敗」とする。

【０２６５】ステータスが「鍵１受信完了」に遷移すると、次に、ユーザ機器６２０は、ユーザ機器認証サーバ６３０に対して電子チケット（ＤＡＳ用）と暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を送信（図３７の処理（１５）に対応）し、データ受信レスポンスを受信する。データ受信レスポンスを受信した場合は、ステータスを「鍵かけかえ要求送信完了」に設定し、データ受信レスポンスを受信しない場合は、処理を中止するか、あるいは同様の処理、ここでは、電子チケット（ＤＡＳ用）と暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵かけかえ要求送信失敗」とする。ステータスが「鍵かけかえ要求送信完了」である場合にのみ次ステップに進む。

【０２６６】ステータスが「鍵かけかえ要求送信完了」に遷移すると、次に、ユーザ機器６２０は、ユーザ機器認証サーバ６３０から、暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）を受信し、データ検証（図３７の処理（１８）、（１９）に対応）を実行する。データ検証に成功した場合は、ステータスを「鍵２受信完了」に設定し、処理を終了する。データ検証に成功しなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵データの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵２受信失敗」とする。

【０２６７】次にチケット換金サーバ６５０のステータス遷移について、図５２を用いて説明する。チケット換金サーバ６５０は、電子チケットによる配分権を持つエンティティからの電子チケットを受信（図３７の処理（２２）、（２７）に対応）することで処理が開始される。チケット換金サーバ６５０は、受信チケットを検証し、検証に成功した場合は、ステータスを「電子チケット受信完了」に設定し、データ検証により正当なデータであるとの判定がなされなかった場合等には、処理を中

止するか、あるいは同様の処理、ここでは、チケットの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「電子チケット受信失敗」とする。ステータスが「電子チケット受信完了」である場合にのみ次ステップに進む。

【０２６８】ステータスが「電子チケット受信完了」に遷移すると、次に、チケット換金サーバ６５０は、電子チケットに基づく換金処理を実行する。換金処理は、予め登録されている利益配分エンティテイ、例えば配信サーバを管理するコンテンツプロバイダ（ＣＰ）の管理口座、あるいは電子マネー口座等に、電子チケット（ＣＰ用）に設定された金額をユーザ機器の管理ユーザの口座から振り替える処理、あるいは既にチケット発行サーバがユーザからの前払い預り金として受領しているチケット発行サーバ管理口座からコンテンツプロバイダ（ＣＰ）の管理口座にチケットに設定された金額を振り替える処理として行なわれる。換金処理が完了するとステータスを「換金処理完了」に設定し、換金処理が実行できなかった場合には、処理を中止し、ステータスを「換金処理失敗」とする。

【０２６９】ステータスが「換金処理完了」に遷移すると、次に、チケット換金サーバ６５０は、チケットを送信してきたエンティテイに対して、換金処理レポートを送信（図３７の処理（２４）、（２９）に対応）し、各エンティテイからのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「換金レポート送信完了」に設定し、処理を終了する。データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、換金レポートの送信処理を所定回数繰り返した後、処理を中止し、ステータスを「換金レポート送信失敗」とする。チケット換金サーバ６５０は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【０２７０】図５３にチケット発行体によって発行されるチケットを流通させることによりコンテンツ料金の精算処理を行なう具体的構成例を示す。ユーザ機器８０２からチケット発行体８０１に対してコンテンツ購入要求があると、チケット発行体は、コンテンツの取り引きに関する課金処理、電子チケット発行処理を実行する。これらの処理は、例えば予め登録されているユーザ口座、あるいは電子マネー口座等に基づいて設定されるユーザの取り引き金額限度内の電子チケットを発行する処理として実行される。図５３に示す例では、コンテンツ購入代金として１，０００円分の電子チケットをチケット発行体がユーザ機器に対して発行する。

【０２７１】図５３の例では、コンテンツ料金１０００円の配分は、図上部に示すように、チケット発行体としてのショップが販売手数料としてのショップ利益として３００円、コンテンツ配信のシステム運営者であるライセンスホルダ（ユーザ機器認証サーバ）８０３がライセンス料として１００円、コンテンツ製作者（配信サーバ）がコンテンツ料として６００円を、それぞれ受領する設定であるとする。

【０２７２】ユーザ機器からの購入要求を受領したチケット発行体８０１は、コンテンツＩＤからコンテンツ料金の配分比率の設定情報を求め、複数の料金配分先がある場合は、それぞれの電子チケットを発行する。図５３の例では、ライセンスホルダ８０３に対するセイセンス料、１００円の配分料金を設定した電子チケットと、コンテンツ製作者に対するコンテンツ料、６００円のチケットをユーザ機器８０２に配信する。配信する電子チケットには、チケット発行体の署名が生成される。

【０２７３】ユーザ機器８０２は、ライセンスホルダ８０３、コンテンツ製作者８０４それぞれに各電子チケットを送信する。ライセンスホルダ８０３、コンテンツ製作者８０４は、受領した電子チケットを検証して、正当なチケットであることを確認した後、銀行（チケット換金サーバ）８０５にチケットを送信し、換金サーバにおいても署名検証を実行し、正当なチケットであることを確認してそれぞれの配分料金の換金（ｅｘ．振替処理）を行なう。なお、銀行（チケット換金サーバ）において実行するチケットの署名検証は、電子チケットに対して生成されたチケット発行体の署名の検証である。また、チケットに含まれる購入要求データのユーザ機器署名の検証も実行する。

【０２７４】さらに、チケットの送信主体であるコンテンツ製作者、ライセンスホルダが電子チケットを含む送信データに対して署名を生成し、これらの署名についても銀行（チケット換金サーバ）が署名検証を実行する構成としてもよい。

【０２７５】図５３の構成では、チケット発行体（ショップ）８０１自身もコンテンツ料金の一部３００円分の自己の電子チケットを銀行（チケット換金サーバ）８０５に送付して換金を行なう構成である。

【０２７６】これらの各電子チケットの換金処理により、確実にコンテンツ料金の配分が実行される。コンテンツ製作者８０４は、電子チケットをユーザ機器８０２から受領して検証した後、コンテンツ鍵Ｋｃで暗号化した暗号化コンテンツと、コンテンツ鍵Ｋｃをライセンスホルダ（ユーザ機器認証サーバ）の公開鍵ＫｐＤＡＳで暗号化した暗号化コンテンツ鍵：ＫｐＤＡＳ（Ｋｃ）をユーザ機器８０２に送信する。

【０２７７】ユーザ機器８０２は、コンテンツ制作者８０４から受領した暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を電子チケット（ＤＡＳ）とともに、ライセンスホルダ８０３に送信する。ライセンスホルダは、電子チケットの検証の後、暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）の鍵かけかえ処理を実行し、ユーザ機器の公開鍵ＫｐＤＥＶでコンテンツ鍵を暗号化して、ＫｐＤＥＶ（Ｋｃ）を生成してユーザ機器８０２に送信する。ユーザ機

器８０２は、ＫｐＤＥＶ（Ｋｃ）を自己の秘密鍵ＫｓＤＥＶで復号してコンテンツ鍵Ｋｃを得ることができる。またコンテンツ鍵をデバイスに格納する場合は、自己の保存鍵Ｋｓｔｏで暗号化して保存する。

【０２７８】上述したように、チケット発行体によって発行するチケットを受信し、正当なチケットであることを条件として配信サーバ（ｅｘ．コンテンツ製作者）が暗号化コンテンツと暗号化コンテンツ鍵をユーザ機器に送信し、一方、ライセンスホルダ（ユーザ認証機器）が、同様に電子チケットを受領し、正当なチケットであることを条件として暗号化コンテンツ鍵のかけかえを行なってユーザ機器に配信する構成としたことにより、電子チケットに基づく確実なコンテンツ料金の配分が実行され、ユーザ機器においてコンテンツの利用が可能となる。

【０２７９】［３．ログ収集サーバによるコンテンツ配信管理］次に、ユーザ機器がコンテンツの購入を行なった事実をユーザ機器にログとして蓄積し、ログの回収をシステム運営者が行なうことにより、コンテンツの流通実体を正確に把握可能としたコンテンツ配信システムについて説明する。

【０２８０】図５４にログ回収システムを持つコンテンツ配信形態のシステム構成を示す。図５４のコンテンツ配信システムは、ユーザ機器に対するコンテンツの配信サービスを行なうショップサーバ（ＳＨＯＰ）９０１、ショップサーバ９０１からのコンテンツ配信を受信するユーザ機器（ＤＥＶＩＣＥ）９０２、さらに、正当なコンテンツ取り引き管理のためのログ管理サーバとして機能するログ収集サーバ９０３を主構成要素とし、コンテンツの提供者としてのコンテンツプロバイダ９０５と、コンテンツプロバイダ９０５から提供されるコンテンツに対してコンテンツの利用制限情報等の各種情報をヘッダとして生成し、ショップサーバに提供するオーサリングサーバ９０４、さらに、各エンティティに対して公開鍵証明書（Ｃｅｒｔ＿ｘｘｘ）を発行する認証局（ＣＡ：Certificate Authority）を有する。

【０２８１】図５４の構成において、コンテンツプロバイダ９０５とオーサリングサーバ９０４は、ショップサーバ９０１に対して、流通対象となるコンテンツを提供するエンティティ構成の一例であり、図５４の形態に限らず、他の様々な態様でショップサーバに対する流通コンテンツの提供がなされる。例えばコンテンツプロバイダから直接ショップサーバにコンテンツが提供されてもよいし、コンテンツの保持者である著作者から複数のサービスプロバイダを介してショップサーバにコンテンツが提供される場合もある。

【０２８２】図５４の構成例は、本発明の説明の理解を容易にするために、コンテンツ売り上げの一部を取得する権利を持つエンティティの1つの代表例としてコンテンツプロバイダ９０５を示したものである。図５４の構成例では、コンテンツプロバイダ９０５は、ログ収集サーバ９０３によって収集されるログに基づいて管理されるコンテンツ売り上げデータの確認により、自己の配分利益を確実に取得することができる。他の利益配分権を有するエンティティがある場合は、そのエンティティが図５４の構成に加わり、ログ収集サーバ９０３によって収集されるログに基づいて自己の配分利益を確認可能である。

【０２８３】図５４の構成において、ショップサーバ９０１は、図１他の構成において説明したと同様の構成であり、暗号処理、通信処理可能な制御部を有し、コンテンツ取り引き処理に伴うステータス管理を実行して、各機器における取り引き処理シーケンスを実行する。また、コンテンツプロバイダ９０５とオーサリングサーバ９０４も暗号処理、通信処理可能な制御部を有し、コンテンツ取り引き処理に伴うステータス管理を実行して、各機器における取り引き処理シーケンスを実行する。

【０２８４】（ユーザ機器）ユーザ機器９０２は、先に図７を用いて説明した構成と同様であり、暗号処理、通信処理可能な制御手段２３０（図７参照）を有する。ただし、本実施例では、制御手段２３０は、コンテンツ購入処理毎にログデータを生成し、購入管理データベース２２０中に生成したログデータを格納する。

【０２８５】ユーザ機器９０２において生成され格納されるログデータの構成例を図５５に示す。図５５には、ログデータの例を２つ示している。（Ａ）構成例１は、ユーザ機器９０２がショップサーバ９０１との取り引きにより取得したコンテンツの識別子であるコンテンツＩＤ、ユーザ機器の識別子であるユーザ機器ＩＤ（ＩＤ＿ＤＥＶ）、取り引きを行なったショップの識別子であるショップＩＤ（ＩＤ＿ＳＨＯＰ）、取り引きの日時を示す日付情報が含まれ、これらのデータに対するユーザ機器の署名（Ｓｉｇ．ＤＥＶ）が生成されている。ログ収集サーバはユーザ機器から受信する購入ログの電子署名の検証処理を実行する。（Ｂ）構成例２は、販売確認データとコンテンツの受領日時データに対してユーザ機器の署名（Ｓｉｇ．ＤＥＶ）が生成された構成である。販売確認データは、ショップサーバ９０１がユーザ機器９０２からのコンテンツ購入要求に基づいて生成するコンテンツの販売を実行したことを示すデータである。販売確認データについては、後段でさらに説明する。

【０２８６】ユーザ機器９０２は、コンテンツ購入処理に際して、例えば図５５に示すログデータを生成しユーザ機器内に格納する。格納されたログデータは、ログ収集サーバ９０３に送信される。ユーザ機器は自己の公開鍵証明書の更新処理実行時に、その間に蓄積したログデータをログ収集サーバ９０３に送信する。これらの処理シーケンスについては、フローを用いて後段で詳細に説明する。

【０２８７】（ログ収集サーバ）ログ収集サーバ９０３

は、図５６に示す構成を有する。ログ収集サーバは、収集ログ管理データベース９０３１を有する。収集ログ管理データベース９０３１は、様々なユーザ機器から受領するログデータ（図５５参照）を格納するデータベースである。

【０２８８】ログ収集サーバ９０３は、ユーザ機器９０２、ショップサーバ９０１等との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段９０３２を有する。制御手段９０３２は、先に説明したショップサーバ等の制御手段と同様、暗号処理手段、通信処理手段としての機能も有する。その構成は、図４を用いて説明した構成と同様である。制御手段９０３２の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。ログ収集サーバ９０３が格納する暗号鍵等の暗号処理用データとしては、ログ収集サーバ９０３の秘密鍵：ＫｓＬＯＧ、ログ収集サーバ９０３の公開鍵証明書Ｃｅｒｔ＿ＬＯＧ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡがある。

【０２８９】ログ収集サーバ９０３は、ユーザ機器９０２からのログデータ受領と引き換えに、公開鍵証明書の発行手続き処理を実行する。具体的には、ユーザ機器９０２から更新用の公開鍵を受領して、受領した公開鍵を認証局９０６に転送して、ユーザ機器の公開鍵証明書の発行要求を行ない、認証局９０６の発行した公開鍵証明書を受領してユーザ機器９０２に送信する。この一連の処理については、フローを用いて後段で詳細に説明する。

【０２９０】（コンテンツ購入処理）本実施例における処理は、図５４の上段に示すように、

Ａ．コンテンツ購入処理

Ｂ．ログ送信、公開鍵証明書更新処理

Ｃ．コンテンツ販売準備処理

Ｄ．売り上げ確認処理

の４つの処理に分類される。以下、これらの各処理についてフローを用いて説明する。

【０２９１】（Ａ．コンテンツ購入処理）コンテンツ購入処理について、図５７、図５８のフローを用いて説明する。図５７、図５８においては、左側にユーザ機器、右側にショップサーバの処理を示している。まず、図５７に示すように、処理開始時に、ユーザ機器とショップサーバ間において相互認証が実行される（Ｓ１５０１，Ｓ１６０１）。

【０２９２】相互認証処理は、図１３を用いて説明した公開鍵方式に基づく処理として実行される。この相互認証においては、認証局（ＣＡ）９０６の発行する有効期限の設定された公開鍵証明書を用いて行われ、ユーザ機器は、有効期限内の公開鍵証明書を持つことが相互認証を成立させるための条件として求められる。後段で説明するが、公開鍵証明書の更新処理は、ログ収集サーバ９０３に対するログの送信を条件として実行される。

【０２９３】相互認証処理において生成したセッション鍵（Ｋｓｅｓ）は、必要に応じて送信データを暗号化してデータ通信を実行したり、あるいはＫｓｅｓを用いた改竄チェック値（ＩＣＶ：Integrity Check Value）の生成処理に使用される。ＩＣＶの生成については後述する。

【０２９４】相互認証が成立すると、ユーザ機器は、コンテンツ取り引きにおいて適用するトランザクションＩＤを例えば乱数に基づいて生成し、購入要求データを生成（Ｓ１５０２）する。購入要求データのフォーマット例を図５９（Ａ）に示す。

【０２９５】購入要求データには前述のトランザクションＩＤ（ＴＩＤ＿ＤＥＶ）、コンテンツ識別子であるコンテンツＩＤ、ユーザ機器の識別子であるユーザ機器ＩＤ（ＩＤ＿ＤＥＶ）、コンテンツ価格である表示価格、さらに購入依頼日時を含み、これらのデータに対するユーザ機器の署名（Ｓｉｇ．Ｄｅｖ）を生成した構成である。

【０２９６】さらに、ユーザ機器は、購入要求データの改竄チェック値（ＩＣＶ１）を生成して、ショップサーバに送信（Ｓ１５０３）する。改竄チェック値（ＩＣＶ）は、改竄チェック対象データに対するハッシュ関数を用いて計算され、ＩＣＶ＝ｈａｓｈ（Ｋｉｃｖ，Ｃ１，Ｃ２，…）によって計算される。ＫｉｃｖはＩＣＶ生成キーである。Ｃ１，Ｃ２は改竄チェック対象データの情報であり、改竄チェック対象データの重要情報のメッセージ認証符号（ＭＡＣ：Message authentication Code）が使用される。

【０２９７】ＤＥＳ暗号処理構成を用いたＭＡＣ値生成例を図６０に示す。図６０の構成に示すように対象となるメッセージを８バイト単位に分割し、（以下、分割されたメッセージをＭ１、Ｍ２、・・・、ＭＮとする）、まず、初期値（Initial Value（以下、ＩＶとする））とＭ１を排他的論理和する（その結果をＩ１とする）。次に、Ｉ１をＤＥＳ暗号化部に入れ、鍵（以下、Ｋ１とする）を用いて暗号化する（出力をＥ１とする）。続けて、Ｅ１およびＭ２を排他的論理和し、その出力Ｉ２をＤＥＳ暗号化部へ入れ、鍵Ｋ１を用いて暗号化する（出力Ｅ２）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたＥＮがメッセージ認証符号（ＭＡＣ（Message Authentication Code））となる。なお、メッセージとしては、検証対象となるデータを構成する部分データが使用可能である。

【０２９８】このようなチェック対象データの改竄チェック値（ＩＣＶ）は、ＩＣＶ生成キーＫｉｃｖを用いて生成されたＭＡＣ値として構成される。改竄のないことが保証された例えばデータ送信側がデータ生成時に生成したＩＣＶと、データ受信側が受信データに基づいて生

成したＩＣＶとを比較して同一のＩＣＶが得られればデータに改竄のないことが保証され、ＩＣＶが異なれば、改竄があったと判定される。

【０２９９】ここでは、ＩＣＶ生成キーとして相互認証時に生成したセッション鍵：Ｋｓｅｓを使用する。ユーザ機器は、セッション鍵：Ｋｓｅｓを適用して購入要求データ（図５９（Ａ）参照）の改竄チェック値（ＩＣＶ１）を生成して、購入要求データ＋ＩＣＶ１をショップサーバに送信する。

【０３００】ショップサーバは、ＩＣＶ１の検証、すなわち、受信データに基づいてセッション鍵：Ｋｓｅｓを適用して改竄チェック値ＩＣＶ１'を生成して、受信したＩＣＶ１＝ＩＣＶ１'が成立するか否かを判定する。成立した場合は、改竄なしと判定する。さらに、ショップサーバは、購入要求データの署名検証（Ｓ１６０３）を行なう。署名検証は、ユーザ機器の公開鍵を用いて行なう。公開鍵はユーザ機器の公開鍵証明書Ｃｅｒｔ＿ＤＥＶから取り出されるものであり、有効期限内の公開鍵証明書であることが条件となる。有効期限の切れた公開鍵証明書は、ショップサーバにおいて署名検証に使用されず、購入依頼ＮＧとなる。ＩＣＶのチェック、署名検証いずれもＯＫであれば、ショップサーバは、販売確認データを生成（Ｓ１６０４）する。

【０３０１】販売確認データは、例えば図５９の（Ｂ）に示すデータ構成を持つ。ショップサーバの生成したトランザクションＩＤ（ＴＩＤ＿ＳＨＯＰ）、ショップの識別子であるショップＩＤ（ＩＤ＿ＳＨＯＰ）、販売日時、コンテンツ販売に対する運営者手数料情報、ここで運営者とは、例えば、コンテンツ販売システムの管理エンティテイ（ＳＨ：システムホルダ）であり、図５４では、ログ収集サーバ９０３を管理するエンティテイである。

【０３０２】さらに、ＣＰ（コンテンツプロバイダ）売り上げ分配情報、これは、コンテンツの売り上げに対するコンテンツプロバイダの配分を示す情報である。さらに、購入要求データ（図５９（Ａ）参照）を含み、これらのデータにショップの署名（Ｓｉｇ．ＳＨＯＰ）が生成された構成である。

【０３０３】図５９（Ｂ）の販売確認データフォーマットは、コンテンツの売り上げに対して運営者（ＳＨ：システムホルダ）と、コンテンツプロバイダ（ＣＰ）との２つのエンティテイの配分情報のみを記録しているが、この他にも、コンテンツ売り上げの配分先エンティテイが存在する場合は、それらの各エンティテイの配分情報も格納する。

【０３０４】ＩＣＶのチェック、署名検証いずれもＯＫであり、販売確認データを生成（Ｓ１６０４）すると、ショップサーバは購入を承諾するメッセージを含む購入ＯＫデータにセッション鍵Ｋｓｅｓを用いて改竄チェック値（ＩＣＶ２）を生成付加してユーザ機器に送信（Ｓ１６０５）する。ＩＣＶのチェック、署名検証いずれかがＮＧであると、ショップサーバは購入を拒否するメッセージを含む購入ＮＧデータにセッション鍵Ｋｓｅｓを用いて改竄チェック値（ＩＣＶ２）を生成付加してユーザ機器に送信（Ｓ１６０６）する。

【０３０５】さらに、ショップサーバは、購入ＯＫデータをユーザ機器に送信した場合は、販売確認データ（図５９（Ｂ）参照）と、ヘッダ（コンテンツの利用情報等を含む各種コンテンツ関連情報）に対してセッション鍵Ｋｓｅｓを用いて改竄チェック値（ＩＣＶ３）を生成したデータとコンテンツとをユーザ機器に送信（Ｓ１６０７）する。

【０３０６】ユーザ機器は、コンテンツおよび、購入要求応答データ（ＯＫまたはＮＧ）＋ＩＣＶ２を受信（Ｓ１５０４）し、ＩＣＶ２の検証を行ない、購入要求応答を確認（Ｓ１５０５）する。ＩＣＶ２によりデータ改竄なしと判定され、購入が受け入れられた（ＯＫ）であるときは、販売確認データ（図５９（Ｂ）参照）と、ヘッダ（コンテンツの利用情報等を含む各種コンテンツ関連情報）＋ＩＣＶ３を受信（Ｓ１５０６）し、ＩＣＶ３の検証、販売確認データの署名検証を行ないいずれもＯＫである場合は、コンテンツ受信ＯＫのレスポンスにＩＣＶ４を生成してショップサーバに送信する。

【０３０７】ステップＳ１５０７の判定がＮｏである場合は、ステップＳ１５０９において、コンテンツ受信ＮＧのレスポンスにＩＣＶ４を生成してショップサーバに送信する。

【０３０８】ショップサーバは、コンテンツ受信ＯＫまたはＮＧ＋ＩＣＶ４を受信（（Ｓ１６０８）し、ＩＣＶ４の検証を行ない（Ｓ１６１１）、さらにユーザ機器からの応答がコンテンツ受信ＯＫである場合は、ユーザに対するコンテンツの課金処理を実行（Ｓ１６１３）する。この課金処理は、前実施例と同様、例えば、ユーザの取り引き口座、あるいはクレジットカード指定口座からコンテンツ料金を受領する処理である。課金処理が終了すると、課金終了メッセージにＩＣＶ５を生成してユーザ機器に送信（Ｓ１６１４）する。ステップＳ１６１１、またはＳ１６１２の判定のいずれかがＮｏである場合は、ステップＳ１６１５において課金未了メッセージにＩＣＶ５を生成してユーザ機器に送信する。

【０３０９】課金終了（または未了）メッセージ＋ＩＣＶ５を受信したユーザ機器は、ＩＣＶ５の検証を実行し、さらに課金が無事終了したかを判定し、課金が済んだことを確認すると、購入ログ（図５５参照）を生成して自デバイスのメモリに保存の後、コンテンツの利用を行なう。ステップＳ１５１２、またはＳ１５１３の判定のいずれかがＮｏである場合は、ステップＳ１５１４においてショップサーバから受領したヘッダ、コンテンツを削除する処理を行なう。

【０３１０】次に、図６１、図６２を用いてユーザ機器

と、ログ収集サーバ間で行われる鍵更新処理と、ログ送信処理とについて説明する。図６１、図６２の左側にユーザ機器の処理、右側にログ収集サーバの処理を示す。この処理は、コンテンツをショップサーバから購入するユーザ機器がユーザ機器に格納されたユーザ機器の公開鍵証明書を更新する際に実行される。ユーザ機器の公開鍵証明書には有効期限が設定されており、一定期間毎に更新処理を実行することが必要となる。図６１の処理から説明する。

【０３１１】まず、ユーザ機器とログ収集サーバは、相互認証を実行（Ｓ１５２１，Ｓ１７２１）しセッション鍵の生成を行なう。ユーザ機器は認証成立を条件として、ユーザ機器デバイス内のメモリに格納された購入ログを取り出して、購入ログに対してセッション鍵Ｋｓｅｓで改竄チェック値（ＩＣＶ１）を生成して購入ログ＋ＩＣＶ１をログ収集サーバに送信（Ｓ１５２２）する。

【０３１２】ログ収集サーバは、購入ログ＋ＩＣＶ１を受信（Ｓ１７２２）し、ＩＣＶ１の検証を実行（Ｓ１７２３）し、検証ＯＫの場合は、ログをデータベース内に保存（Ｓ１７２４）する。なお、ログ収集サーバは、さらに、購入ログ中のユーザ機器の電子署名の検証処理を行なって、データ改竄の有無を更にチェックする構成としてもよい。ログ収集サーバは、さらに、ログ受信ＯＫデータにセッション鍵Ｋｓｅｓで改竄チェック値（ＩＣＶ２）を生成し、ログ受信ＯＫデータ＋ＩＣＶ２をユーザ機器に送信（Ｓ１７２５）する。ステップＳ１７２３のＩＣＶ１の検証ＮＧであったときは、ログ受信ＮＧデータにセッション鍵Ｋｓｅｓで改竄チェック値（ＩＣＶ２）を生成し、ログ受信ＮＧデータ＋ＩＣＶ２をユーザ機器に送信（Ｓ１７２６）する。

【０３１３】ユーザ機器は、ログ受信データ＋ＩＣＶ２を受信（Ｓ１５２３）し、ＩＣＶ２の検証ＯＫ、ログ受信ＯＫ（Ｓ１５２４）である場合は、更新用の公開鍵（ＫｐＤＥＶ）と秘密鍵（ＫｓＤＥＶ）のペアを生成（Ｓ１５２５）し、生成した公開鍵（ＫｐＤＥＶ）に改竄チェック値（ＩＣＶ３）を生成付加してログ収集サーバに送信（Ｓ１５２６）する。

【０３１４】ログ収集サーバは、公開鍵（ＫｐＤＥＶ）＋ＩＣＶ３をユーザ機器から受信する（Ｓ１７２７）と、ＩＣＶ３の検証を実行（Ｓ１７３１）し、検証ＯＫである場合は公開鍵受信ＯＫメッセージに対するＩＣＶ４を生成付加してユーザ機器に送信（Ｓ１７３２）する。ＩＣＶ３の検証がＮＧである場合は公開鍵受信ＮＧメッセージにＩＣＶ４を生成付加してユーザ機器に送信（Ｓ１７３３）する。

【０３１５】さらに、ログ収集サーバは、公開鍵受信ＯＫメッセージに対するＩＣＶ４を生成付加してユーザ機器に送信（Ｓ１７３２）した場合、発行局（ＣＡ）に対して受領公開鍵とともに、公開鍵証明書の発行を要求して、ユーザ機器の更新された公開鍵証明書（Ｃｅｒｔ＿ＤＥＶ）を取得（Ｓ１７３４）し、さらに、更新された公開鍵証明書（Ｃｅｒｔ＿ＤＥＶ）に対する改竄チェック値ＩＣＶ５を生成付加してユーザ機器に送信（Ｓ１７３５）する。

【０３１６】ユーザ機器は、公開鍵受信結果（ＯＫまたはＮＧ）＋ＩＣＶ４を受信した後、ＩＣＶ４の検証を行ない、ＩＣＶ４検証ＯＫであり、公開鍵受信ＯＫ（Ｓ１５３２）である場合には、更新された公開鍵証明書＋ＩＣＶ５の受信（Ｓ１５３３）を実行し、ＩＣＶ５の検証、受信した公開鍵証明書の検証（Ｓ１５３４）を実行する。いずれの検証もＯＫである場合は、公開鍵証明書内の公開鍵を取り出して、自己の送信した公開鍵との比較（Ｓ１５３５）を行ない、一致した場合は更新用に生成した秘密鍵、および受領した公開鍵証明書をユーザ機器内のメモリに保存（Ｓ１５３６）し、ログ（ログ収集サーバに送付済みのログ）の消去処理（Ｓ１５３７）を実行する。

【０３１７】ステップＳ１５３２、Ｓ１５３４、Ｓ１５３５のいずれかの判定がＮｏである場合は、有効な公開鍵証明書の更新処理は実行されず、処理は終了する。

【０３１８】次に、コンテンツプロバイダとログ収集サーバ間で実行されるコンテンツ売り上げ確認処理について図６３のフローに基づいて説明する。ログ収集サーバは、ユーザ機器から受領する購入ログに基づいてコンテンツ料金の１または複数の料金受領エンティテイに対する料金配分情報を管理し、料金受領エンティテイからの売り上げ確認要求に応じて料金配分情報に基づく応答処理を実行する。ログ収集サーバは、購入ログに含まれるコンテンツＩＤと予めログ収集サーバが保有するコンテンツ料金配分情報から、コンテンツの売り上げに基づく料金受領エンティテイの売り上げを算出することができる。なお、図５５（Ｂ）に示す販売確認データを格納したログを受領する構成である場合は、販売確認データに含まれる分配情報に基づいて料金受領エンティテイの売り上げを算出することができる。

【０３１９】まず、コンテンツプロバイダとログ収集サーバ間において、相互認証（Ｓ１５２１，Ｓ１７２１）が実行され、セッション鍵Ｋｓｅｓが生成される。ログ収集サーバは、相互認証の成立を条件として、コンテンツプロバイダ（ＣＰ）の公開鍵証明書Ｃｅｒｔ＿ＣＰからコンテンツプロバイダの識別子ＩＤ＿ＣＰを取り出し（Ｓ１７２２）、ＩＤ＿ＣＰに対応する売り上げデータをデータベースに格納したログ情報に基づいて生成（Ｓ１７２３）する。収集したログデータには、前述したようにコンテンツプロバイダの配分情報が格納されており、ログデータに基づいて各コンテンツプロバイダの配分料金が求められる。さらに、ログ収集サーバは、売り上げデータに対する改竄チェック値ＩＣＶ１を生成付加してコンテンツプロバイダ（ＣＰ）に送信（Ｓ１７２４）する。

【０３２０】コンテンツプロバイタ（ＣＰ）は、ログ収集サーバから売り上げデータ＋ＩＣＶ１を受信（Ｓ１５２２）し、ＩＣＶ１の検証を行なってデータ改竄のないことを確認して（Ｓ１５２３）売り上げデータをメモリに保存（Ｓ１５２４）する。ＩＣＶ１の検証を行なってデータ改竄ありの場合は、メモリに対するデータ保存を実行せず、処理を終了する。この場合は、再度、ログ収集サーバに対する売り上げデータ要求を行なう。

【０３２１】次に、ショップサーバとログ収集サーバ、コンテンツプロバイダ間で実行される売り上げ報告処理について図６４、図６５の処理フローに基づいて説明する。ショップサーバは、コンテンツの売り上げデータを管理し、ログ収集サーバに対して、所定期間内の全売り上げてデータまたは、料金受領エンティテイ毎の売り上げデータを送信する処理を実行する。図６４は、ショップサーバが実行したコンテンツ販売処理全体の売り上げを一括してログ収集サーバに送信する処理であり、図６５の処理は、ショップサーバが実行したコンテンツ販売処理中、特定のコンテンツプロバイダの提供したコンテンツに関する売り上げを選択してコンテンツプロバイダに送信する処理である。

【０３２２】図６４の売り上げ一括報告処理から説明する。まず、ショップサーバとログ収集サーバ間において、相互認証（Ｓ１６３１，Ｓ１７３１）が実行され、セッション鍵Ｋｓｅｓが生成される。ショップサーバは、相互認証の成立を条件として、所定期間の全売り上げデータをデータベースから取り出し、全売り上げデータに対する改竄チェック値ＩＣＶ１を生成付加してログ収集サーバに送信（Ｓ１６３２）する。

【０３２３】ログ収集サーバは、ショップサーバから全売り上げデータ＋ＩＣＶ１を受信（Ｓ１７３２）し、ＩＣＶ１の検証を行なってデータ改竄のないことを確認して（Ｓ１７３３）、売り上げデータをメモリに保存（Ｓ１７３４）する。ＩＣＶ１の検証を行なってデータ改竄ありの場合は、メモリに対するデータ保存を実行せず、処理を終了する。この場合は、再度、ショップサーバに対する売り上げデータ要求を行なう。

【０３２４】図６５の特定コンテンツプロバイダ売り上げ報告処理について説明する。まず、ショップサーバとコンテンツプロバイダ間において、相互認証（Ｓ１６４１，Ｓ１７４１）が実行され、セッション鍵Ｋｓｅｓが生成される。ショップサーバは、相互認証の成立を条件として、相互認証で得られたコンテンツプロバイダの公開鍵証明書Ｃｅｒｔ＿ＣＰからコンテンツプロバイダの識別子であるＩＤ＿ＣＰを取り出し（Ｓ１６４２）、取り出したＩＤ＿ＣＰに基づいて、売り上げデータの検索を行ない、その特定コンテンツプロバイダの提供コンテンツの売り上げデータを取得（Ｓ１６４３）する。さらに売り上げデータに対する改竄チェック値ＩＣＶ１を生成付加してログ収集サーバに送信（Ｓ１６４４）する。

【０３２５】ログ収集サーバは、ショップサーバから全売り上げデータ＋ＩＣＶ１を受信（Ｓ１７４２）し、ＩＣＶ１の検証を行なってデータ改竄のないことを確認して（Ｓ１７４３）、売り上げデータをメモリに保存（Ｓ１７４４）する。ＩＣＶ１の検証を行なってデータ改竄ありの場合は、メモリに対するデータ保存を実行せず、処理を終了する。この場合は、再度、ショップサーバに対する売り上げデータ要求を行なう。

【０３２６】本実施例の構成によれば、ユーザ機器の公開鍵証明書の更新処理に応じてコンテンツ購入ログデータを収集することが可能となり、ログ収集サーバを管理するシステム運営者（ＳＨ：System Holder）は、コンテンツ売り上げ状況を確実に把握することが可能となる。ユーザ機器の公開鍵証明書は、ショップサーバとの相互認証処理において必要であり、有効な期限の設定された公開鍵証明書を有することがコンテンツ購入を実行するための条件となる。また、ユーザ機器からの購入要求データ等に付加される署名の検証もユーザ機器の公開鍵証明書から取り出される公開鍵によって実行されることになり、有効な期限の設定された公開鍵証明書を有することが署名検証においても必要となる。従って、ユーザ機器は、コンテンツ購入を行なうためには、ログデータをログ収集サーバに送信し、公開鍵証明書の更新を行ない有効な期限を持つ公開鍵証明書を有することが必要となる。公開鍵証明書の有効期限を例えば１ヶ月、または３ヶ月等に設定することにより、ログ収集サーバを管理するシステム運営者（ＳＨ：System Holder）は、各設定機関毎の蓄積ログを確実に収集することができる。

【０３２７】上述したように、システム運営者の管理するログ収集サーバにより確実にユーザ機器からのログデータが収集され、コンテンツ売り上げ状況を管理することが可能となる。さらに、ログデータ中の売り上げ配分情報に基づいて、コンテンツ売り上げをコンテンツプロバイダ等の売り上げ利益取得権利者に対して正確な配分が可能となる。

【０３２８】また、本実施例では、各エンティテイ間において通信されるデータに相互認証時に生成したセッション鍵Ｋｓｅｓを改竄チェック値（ＩＣＶ）の生成鍵として用い、送信データにＩＣＶを付加して通信する構成としたので、通信データの安全性がさらに高まることになる。

【０３２９】なお、上述した実施例では、ユーザ機器とショップサーバ間の相互認証処理、署名生成、署名検証処理のいずれも実行する構成として説明したが、いずれかのみの処理、すなわち、相互認証のみ、あるいは署名生成、署名検証処理のみを実行する構成として、いずれかにおいて有効期限内の公開鍵証明書の利用を必須とする構成としてもよい。

【０３３０】［４．属性データを記録した公開鍵証明書または属性証明書利用構成］次に、属性データを記録し

た公開鍵証明書または属性証明書の利用構成について説明する。例えば上述したコンテンツ配信構成において、悪意のショップ運営者がユーザ機器になりすましてコンテンツの架空取り引きを実行したり、あるいはコンテンツプロバイダとショップ間における架空コンテンツ取り引きを行なう可能性がある。また、正当な取り引きを実行しようとするユーザ機器がショップサーバであると信じて通信を開始し、ショップサーバ相手のコンテンツ購入要求を実行して、例えばクレジット口座番号の送信処理を実行するような場合、相手がショップサーバになりすました不正なサーバであるような場合は、ユーザ機器からクレジット口座番号を不正に取得する等の処理が実行されるおそれがある。さらに、ユーザ機器がショップになりすまして、他のユーザ機器に対してコンテンツの架空販売を行なうなどの処理を行なう可能性も否定できない。このような事態が発生すると、システム運営者は正確なコンテンツ配信実体を把握することが困難となる。

【０３３１】このような正規なコンテンツ配信ルート以外の架空取引等を防止する構成として、以下、属性データを記録した公開鍵証明書または属性証明書利用構成を説明する。

【０３３２】属性データとは、ユーザ機器（ＤＥＶＩＣＥ）、ショップ（ＳＨＯＰ）、コンテンツプロバイダ（ＣＰ）、サービス運営者（ＳＨ）、公開鍵証明書、属性証明書の発行審査を行なう登録局等、コンテンツ配信システムを構成するエンティテイの種別を識別するデータである。

【０３３３】属性データの構成例として、属性データの内容を示すテーブルを図６６に示す。図６６に示すように、異なるコードが各エンティテイに割り当てられる。例えば、ユーザ機器あるいはショップ等から公開鍵証明書、属性証明書の発行要求を受けつけ、審査を行なう登録局には「００００」、コンテンツ配信システム上で流通するコンテンツに対するライセンスを徴収するシステムホルダとしてのサービス運営者には「０００１」が属性コードとして割り振られる。上述した例では、サービス運営者は鍵かけかえ処理を実行するユーザ機器認証サーバを管理するエンティテイであったり、また、ログ情報を収集するログ情報収集サーバを管理するエンティテイである。

【０３３４】さらに、ユーザ機器に対してコンテンツを販売するショップとしてのコンテンツ販売者には、「０００２」、ショップ（コンテンツ販売者）からの要求に応じてコンテンツをユーザに配信する配信サーバの運営エンティテイであるコンテンツ配信者には、「０００３」、コンテンツを購入し利用するユーザ機器には「０００４」のコードが割り当てられる。この他にもコンテンツ配信に係わるエンティテイに対して、その種類に応じて異なるコードが割り当てられる。なお、ショップに必ずしも１つのコードを割り当てる構成に限らず、役割、機能の異なるショップがある場合には、異なるコードを割り当てて、それぞれを区別可能にしてもよいし、またユーザ機器にも、何らかのカテゴリに応じて異なる属性コードを割り当てる構成としてもよい。

【０３３５】上述した属性情報は、公開鍵証明書に含める構成と、公開鍵証明書とは異なる属性証明書を発行し、属性証明書によって属性を識別する構成とがある。属性情報を持つ公開鍵証明書の構成例を図６７に示す。

【０３３６】図６７に示す公開鍵証明書は、証明書のバージョン番号、公開鍵証明書発行局（ＣＡ）が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、発行局の名前、証明書の有効期限、証明書利用者の名前（ｅｘ．ユーザ機器ＩＤ）、証明書利用者の公開鍵、さらに、上述した［００００］，［０００１］…［ｎｎｎｎ］等の属性情報、さらに電子署名を含む。証明書の通し番号は、例えば発行年（４バイト）、月（２バイト）、日（２バイト）、シリアル番号（８バイト）の合計１６バイトとする。利用者名は、登録局の定める識別可能な名前、あるいは乱数、通し番号を用いてもよい。あるいは上位バイトをカテゴリとし、下位バイトを通し番号とする構成としてもよい。

【０３３７】電子署名は、証明書のバージョン番号、公開鍵証明書発行局（ＣＡ）が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、発行局の名前、証明書の有効期限、証明書利用者の名前、証明書利用者の公開鍵、並びに属性データ全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して発行局の秘密鍵を用いて生成したデータである。

【０３３８】公開鍵証明書発行局（ＣＡ）は、図６７に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（これをリボケーション：Revocationと呼ぶ）を行う。

【０３３９】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する発行局の公開鍵ＫｐＣＡを用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の公開鍵証明書発行局の公開鍵を保持している必要がある。

【０３４０】次に図６８に属性情報を持たない公開鍵証明書と、属性証明書のデータ構成を示す。（Ａ）は属性情報を持たない公開鍵証明書であり、図６７に示す公開鍵証明書から属性情報を取り除いたデータ構成であり、公開鍵証明書発行局が発行する。（Ｂ）は属性証明書である。属性証明書は、属性証明書発行局（ＡＡ：Attribute Authority）が発行する。

【０３４１】図６８に示す属性証明書は、証明書のバージョン番号、属性証明書発行局（ＡＡ）が発行する属性証明書に対応する公開鍵証明書の通し番号、これは対応公開鍵証明書の証明書の通し番号と同一であり、両証明書を関連づけるリンクデータとしての機能を持つ。属性証明書によって通信相手の属性を確認しようとするエンティティは、公開鍵証明書とリンクする属性証明書を、公開鍵証明書および属性証明書に共通に格納された公開鍵証明書通し番号に基づいて確認し、公開鍵証明書と同一の公開鍵証明書通し番号を格納した属性証明書から属性情報を取得することができる。通し番号は、例えば発行年（４バイト）、月（２バイト）、日（２バイト）、シリアル番号（８バイト）の合計１６バイトとする。さらに、電子署名に用いたアルゴリズムおよびパラメータ、属性証明書発行局の名前、証明書の有効期限、証明書利用者の名前（ｅｘ．ユーザ機器ＩＤ）、これは、対応する公開鍵証明書の利用者名と同一であり、登録局の定める識別可能な名前、あるいは乱数、通し番号、あるいは上位バイトをカテゴリとし、下位バイトを通し番号としたデータ構成である。さらに、上述した［００００］，［０００１］…［ｎｎｎｎ］等の属性情報、属性証明書発行局（ＡＡ）の電子署名を含む。

【０３４２】電子署名は、証明書のバージョン番号、公開鍵証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、発行局の名前、証明書の有効期限、証明書利用者の名前、並びに属性データ全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して属性証明書発行局の秘密鍵を用いて生成したデータである。

【０３４３】属性証明書発行局（ＡＡ）は、図６８（Ｂ）に示す属性証明書を発行するとともに、有効期限が切れた属性証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（これをリボケーション：Revocationと呼ぶ）を行う。

【０３４４】図６９にコンテンツ取り引きに参加するユーザ機器、ショップサーバがそれぞれ使用する公開鍵証明書を新規に発行する手続きを説明する図を示す。なお、ここでショップサーバ１０１０、ユーザ機器１０２０は、前述の図１他で説明したと同様の構成を持つ。サービス運営体１０３０は、コンテンツ配信全体を管理するシステムホルダ（ＳＨ）であり、前述したコンテンツ鍵のかけかえ処理、あるいはユーザ機器のコンテンツ購入により生成されるログを収集する等の手法により、コンテンツの流通状況を把握する。ここでは、さらに、ショップサーバ１０１０、ユーザ機器１０２０他の公開鍵証明書および属性証明書の発行要求の受付、審査を実行する登録局（ＲＡ：Registration Authority）としての機能も兼ね備える。なお、本例ではサービス運営体１０３０がシステムホルダ（ＳＨ）としての機能と、登録局（ＲＡ）としての機能を持つ構成であるが、これらは別々の独立したエンティティとして構成してもよい。

【０３４５】図６９では、ユーザ機器１０２０における公開鍵証明書の新規発行手続きをＡ１～Ａ８で示し、ショップサーバ１０１０の公開鍵証明書の新規発行手続きをＢ１～Ｂ７で示している。まず、ユーザ機器１０２０における公開鍵証明書の新規発行手続きについて説明する。

【０３４６】（Ａ１）相互認証

まず、ユーザ機器１０２０は、サービス運営体１０３０との間で相互認証を実行する。ただし、この時点でユーザ機器１０２０は、公開鍵証明書を保有していないので、公開鍵証明書を用いた相互認証を実行することはできず、先に図１２を用いて説明した対称鍵暗号方式、すなわち、共有秘密鍵、識別子（ＩＤ）を用いた相互認証処理を実行（詳細は図１２に関する説明を参照）する。

【０３４７】（Ａ２）公開鍵、秘密鍵ペア生成

（Ａ３）公開鍵証明書発行要求

（Ａ４）審査＆公開鍵証明書発行要求

（Ａ５）公開鍵証明書発行要求

相互認証が成立すると、ユーザ機器１０２０は、自己のデバイス内の暗号処理部において、新規に登録する公開鍵と秘密鍵のペアを生成し、生成した公開鍵をサービス運営体１０３０に対して、証明書発行要求とともに送信する。公開鍵証明書発行要求を受信したサービス運営体１０３０は、発行要求を審査し、公開鍵証明書を発行するエンティティとしての要件を満足している場合に、証明書発行要求を公開鍵証明書発行局（ＣＡ）１０４０に対して送信する。なお、ここで発行する公開鍵証明書が図６８（Ａ）に示す属性情報を持つ公開鍵証明書である場合は、サービス運営体１０３０は、証明書発行要求を送信してきたエンティティの属性をＩＤに基づいて判定する。

【０３４８】コンテンツ配信に参加するユーザ機器には、予めユーザ機器識別子（ＩＤ）および秘密情報としての秘密鍵が格納され、これらユーザ機器ＩＤ、秘密鍵はサービス運営体１０３０によって管理された構成であり、サービス運営体１０３０は、ユーザ機器から送信されるＩＤに基づき秘密情報格納データベースを検索し、予め登録済みのユーザ機器ＩＤであることを確認した後、秘密鍵を取り出し、この鍵を用いてユーザ機器と図１２に基づく相互認証を行ない、相互認証に成功した場合にのみコンテンツ配信に参加可能なユーザ機器であることを確認する。

【０３４９】（Ａ６）公開鍵証明書発行

（Ａ７）公開鍵証明書送信

（Ａ８）公開鍵証明書送信

サービス運営体１０３０からの公開鍵証明書発行要求を受信した公開鍵証明書発行局１０４０は、ユーザ機器の公開鍵を格納し、公開鍵証明書発行局１０４０の電子署名を持つ公開鍵証明書（図６７または図６８（Ａ））を

発行し、サービス運営体１０３０に送信する。サービス運営体１０３０は、公開鍵証明書発行局１０４０から受信した公開鍵証明書をユーザ機器１０２０に対して送信する。ユーザ機器は、受信した公開鍵証明書と先ほど（Ａ２）で生成しておいた秘密鍵を自デバイス内に格納し、コンテンツ取り引きの際の相互認証、データ暗号化、復号処理等に使用可能となる。

【０３５０】一方、ショップサーバ１０１０の公開鍵証明書の発行手続きは、基本的にユーザ機器における証明書発行手続きと同様であるが、ショップサーバは、コンテンツの販売を手がけるエンティテイとしてサービス運営体１０３０に認可してもらう手続きが必要となる。従って、ショップサーバ１０１０は、自己の公開鍵とともに、ライセンス申請（図６９、Ｂ２の手続き）を実行することが必要となる。これは、例えばサービス運営体１０３０が定めるポリシーに従ったコンテンツ販売を実行することをショップサーバ１０１０が受諾する処理として実行されるものである。サービス運営体１０３０は、ショップサーバ１０１０がサービス運営体１０３０が定めるポリシーに従ったコンテンツ販売を実行可能であり、ショップサーバ１０１０がポリシーを遵守することを受諾した場合には、ショップに対する公開鍵証明書の発行手続きを進める。公開鍵証明書の発行手続き処理は、上述したユーザ機器の場合と同様である。

【０３５１】次に、公開鍵証明書の更新処理について図７０を用いて説明する。公開鍵証明書は図６７，図６８（Ａ）に示すように有効期限が定められており、公開鍵証明書を使用するエンティテイは有効期限のすぎた証明書は使用できないので、有効期限内に更新処理を実行し、新たな有効期限の設定された公開鍵証明書の発行手続きを行なうことが必要となる。

【０３５２】図７０において、ユーザ機器１０２０における公開鍵証明書の更新手続きをＡ１～Ａ８で示し、ショップサーバ１０１０の公開鍵証明書の更新手続きをＢ１～Ｂ７で示している。まず、ユーザ機器１０２０における公開鍵証明書の更新手続きについて説明する。

【０３５３】（Ａ１）相互認証

まず、ユーザ機器１０２０は、サービス運営体１０３０との間で相互認証を実行する。この時点でユーザ機器１０２０は、現在有効な公開鍵証明書を保有しているので、公開鍵証明書を用いた相互認証を実行する。これは先に図１３を用いて説明した相互認証処理である。なお、すでに手持ちの公開鍵証明書の有効期限がすぎている場合は、新規発行手続きと同様先に図１２を用いて説明した共有秘密鍵、識別子（ＩＤ）を用いた相互認証処理を実行するようにしてもよい。

【０３５４】（Ａ２）新規公開鍵、秘密鍵ペア生成

（Ａ３）公開鍵証明書更新要求

（Ａ４）審査＆公開鍵証明書更新要求

（Ａ５）公開鍵証明書更新要求

相互認証が成立すると、ユーザ機器１０２０は、自己のデバイス内の暗号処理部において、更新用の新規公開鍵と秘密鍵のペアを生成し、生成した公開鍵をサービス運営体１０３０に対して、証明書更新要求とともに送信する。公開鍵証明書更新要求を受信したサービス運営体１０３０は、更新要求を審査し、更新要件を満足している場合に、証明書更新要求を公開鍵証明書発行局（ＣＡ）１０４０に対して送信する。なお、ここで発行する公開鍵証明書が図６８（Ａ）に示す属性情報を持つ公開鍵証明書である場合は、サービス運営体１０３０は、証明書発行要求を送信してきたエンティテイの属性をＩＤに基づいて判定する。

【０３５５】（Ａ６）公開鍵証明書更新

（Ａ７）公開鍵証明書送信

（Ａ８）公開鍵証明書送信

サービス運営体１０３０からの公開鍵証明書更新要求を受信した公開鍵証明書発行局１０４０は、ユーザ機器の新規公開鍵を格納し、公開鍵証明書発行局１０４０の電子署名を持つ公開鍵証明書（図６７または図６８（Ａ））を発行し、サービス運営体１０３０に送信する。サービス運営体１０３０は、公開鍵証明書発行局１０４０から受信した公開鍵証明書をユーザ機器１０２０に対して送信する。ユーザ機器は、受信した公開鍵証明書と先ほど（Ａ２）で生成しておいた秘密鍵を自デバイス内に格納し、コンテンツ取り引きの際の相互認証、データ暗号化、復号処理等に使用可能となる。

【０３５６】一方、ショップサーバ１０１０の公開鍵証明書の更新手続きは、基本的にユーザ機器における証明書更新手続きと同様であるが、前述のライセンス申請の更新（図７０、Ｂ２の手続き）を実行することが必要となる。サービス運営体１０３０が、ショップサーバ１０１０のライセンス更新を認めた場合には、ショップに対する公開鍵証明書の更新手続きを進める。公開鍵証明書の更新手続き処理は、上述したユーザ機器の場合と同様である。

【０３５７】次に、図７１を用いて属性証明書の新規発行手続きについて説明する。属性証明書は、図６８（Ｂ）に示す証明書であり、図６８（Ａ）に示す公開鍵証明書の発行の後、属性証明書が発行される。図７１では、ユーザ機器１０２０における属性証明書の新規発行手続きをＡ１～Ａ７で示し、ショップサーバ１０１０の公開鍵証明書の新規発行手続きをＢ１～Ｂ７で示している。まず、ユーザ機器１０２０における公開鍵証明書の新規発行手続きについて説明する。

【０３５８】（Ａ１）相互認証

まず、ユーザ機器１０２０は、サービス運営体１０３０との間で相互認証を実行する。この時点でユーザ機器１０２０は、すでに公開鍵証明書発行局公開鍵証明書を保有しているので、公開鍵証明書を用いた相互認証を実行する。

【０３５９】（Ａ２）属性証明書発行要求
（Ａ３）審査＆属性証明書発行要求
（Ａ４）属性証明書発行要求
相互認証が成立すると、ユーザ機器１０２０は、サービス運営体１０３０に対して、属性証明書発行要求を送信する。属性証明書発行要求を受信したサービス運営体１０３０は、発行要求を審査し、属性証明書を発行するエンティティとしての要件を満足している場合に、証明書発行要求を属性証明書発行局（ＡＡ）１０５０に対して送信する。なお、ここでサービス運営体１０３０は、証明書発行要求を送信してきたエンティティの属性をＩＤに基づいて判定する。前述したように、コンテンツ配信に参画するユーザ機器には、予めユーザ機器識別子（ＩＤ）が格納され、これらユーザ機器ＩＤはサービス運営体１０３０によって管理された構成であり、サービス運営体１０３０は、ユーザ機器から送信されるＩＤと、予め登録済みのユーザ機器ＩＤと比較参照することにより、コンテンツ配信に参画可能なユーザ機器であることを確認する。

【０３６０】（Ａ５）属性証明書発行
（Ａ６）属性証明書送信
（Ａ７）属性証明書送信
サービス運営体１０３０からの属性証明書発行要求を受信した属性証明書発行局１０５０は、ユーザ機器の属性情報を格納し、属性証明書発行局１０５０の電子署名を持つ属性証明書（図６８（Ｂ））を発行し、サービス運営体１０３０に送信する。サービス運営体１０３０は、属性証明書発行局１０５０から受信した属性証明書をユーザ機器１０２０に対して送信する。ユーザ機器は、受信した属性証明書を自デバイス内に格納し、コンテンツ取り引きの際の属性確認処理に使用する。

【０３６１】一方、ショップサーバ１０１０の属性証明書の発行手続き（Ｂ１～Ｂ７）は、基本的にユーザ機器における証明書発行手続きと同様である。また、属性証明書の更新手続きも新規発行手続きと同様の手続きとなる。

【０３６２】次に、属性証明書による属性確認処理、または公開鍵証明書に格納された属性情報による属性確認処理を伴うコンテンツ取り引きについて説明する。

【０３６３】図７２に相互認証時に併せて属性確認処理を実行する処理構成を示す。図７２の構成は、先に説明した図１のシステム構成と同様である。すなわち、コンテンツの販売を実行するショップサーバ１０１０、コンテンツ購入を実行するユーザ機器１０２０、ユーザ機器認証サーバ１０３０を構成要素とする。ここで、ユーザ機器認証サーバ１０３０は、前述したサービス運営体の管理下にある。図７２の番号（１）から（２０）の順に処理が進行する。各番号順に処理の詳細を説明する。

【０３６４】（１）相互認証および属性確認処理
コンテンツをショップサーバ１０１０から購入しようとするユーザ機器１０２０は、ショップサーバとの間で相互認証処理を行なう。データ送受信を実行する２つの手段間では、相互に相手が正しいデータ通信者であるか否かを確認して、その後に必要なデータ転送を行なうことが行われる。相手が正しいデータ通信者であるか否かの確認処理が相互認証処理である。相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が１つの好ましいデータ転送方式である。公開鍵方式の相互認証処理は、公開鍵証明書の発行局の署名検証の後、相手型の公開鍵を取り出して実行される。詳細は前述の図１３に関する説明を参照されたい。

【０３６５】さらに、本実施例においては、属性確認処理を実行する。ショップサーバ１０１０は、通信相手の公開鍵証明書に属性データが格納されている場合は、その属性がユーザ機器であることを示すデータであることを確認する。公開鍵証明書に属性データが格納されていない場合は、属性証明書を用いて属性の確認を行なう。属性証明書には、属性証明書発行局の秘密鍵を用いて署名がなされているので、属性証明書発行局の公開鍵：ＫｐＡＡを用いて署名検証を実行し、正当な証明書であることを確認し、属性証明書の「通し番号」および／または「利用者（ＩＤ）」が、公開鍵証明書内の「通し番号」および／または「利用者（ＩＤ）」と一致しているか確認した後、証明書内の属性情報を確認する。

【０３６６】一方、ユーザ機器１０２０は、通信相手の公開鍵証明書に属性データが格納されている場合は、その属性がショップであることを示すデータであることを確認する。公開鍵証明書に属性データが格納されていない場合は、属性証明書について、属性証明書発行局の公開鍵：ＫｐＡＡを用いて署名検証を実行し、正当な証明書であることを確認し、属性証明書の「通し番号」および／または「利用者（ＩＤ）」が、公開鍵証明書内の「通し番号」および／または「利用者（ＩＤ）」と一致しているか確認した後、証明書内の属性情報を確認する。

【０３６７】ショップサーバ１０１０は、コンテンツ購入要求主体の公開鍵証明書または属性証明書の属性がユーザ機器であることを確認し、ユーザ機器１０２０は、コンテンツ購入要求先の公開鍵証明書または属性証明書の属性がショップであることを確認して、その後の処理に移行する。

【０３６８】属性確認処理のフローを図７３に示す。図７３（Ａ）は、公開鍵証明書に属性データが格納されている場合の公開鍵証明書を用いた属性確認処理であり、（Ｂ）は、属性証明書を用いた属性確認処理である。

【０３６９】図７３（Ａ）のフローから説明する。まず、ステップＳ２１０１において、公開鍵証明書を用いた相互認証処理を実行（図１３参照）し、認証が成立したことを条件として（Ｓ２１０２の判定Ｙｅｓ）、相手

の公開鍵証明書から属性情報を取り出す。属性情報が正当である場合に（Ｓ２１０４の判定Ｙｅｓ）、相互認証、属性確認が成功したものと判定（Ｓ２１０５）し、その後の処理に移行する。なお、属性が正当であるとは、例えばユーザ機器がショップサーバにアクセスしコンテンツ購入要求を実行しようとしている場合は、属性がショップであれば正当であると判定し、ショップ以外の例えば他のユーザ機器を示す属性コードであれば正当でないと判定する。この判定処理は、例えばショップサーバに対してコンテンツ購入要求を実行する場合は、コンテンツ購入要求処理シーケンス（ｅｘ．実行プログラム）中に属性コード比較処理を実行するステップを含ませ、予めショップに対して付与されたコード［０００２］と、通信相手（エンティテイ）の公開鍵証明書、または属性証明書から取得した属性コードとを比較し、一致すれば正当と判定し、不一致であれば正当でないと判定する。あるいは、通信相手（エンティテイ）の公開鍵証明書、または属性証明書から取得した属性コードをディスプレイに表示するなどして、通信相手として想定したエンティテイに設定された属性コードとを比較してユーザ自身が判定する構成としてもよい。ステップＳ２１０２，Ｓ２１０４で判定がＮｏの場合は、相互認証、属性確認が失敗であると判定（Ｓ２１０６）し、その後の処理を中止する。

【０３７０】属性正当性の判定は、上述のように、ショップに対する処理実行プログラムでは、予めショップに対して付与されたコード［０００２］と、通信相手（エンティテイ）の公開鍵証明書、または属性証明書から取得した属性コードとを比較する処理としてステップが実行され、また、ユーザ機器がユーザ機器認証サーバに対して実行する例えば鍵かけかえ要求処理実行シーケンス（ｅｘ．プログラム）では、予めユーザ機器認証サーバに対して付与されたコード［０００１］と、通信相手（エンティテイ）の公開鍵証明書、または属性証明書から取得した属性コードとを比較する処理としてステップが実行される。その他、ショップとユーザ機器認証サーバ間における通信処理においても、それぞれのエンティテイで通信相手を特定して実行する処理シーケンス（ｅｘ．プログラム）において、予め正当な通信相手として設定された属性コードと、通信相手（エンティテイ）の公開鍵証明書、または属性証明書から取得した属性コードとを比較する処理としてステップが実行される。

【０３７１】次に、図７３（Ｂ）の属性証明書を適用したフローについて説明する。まず、ステップＳ２２０１において、公開鍵証明書を用いた相互認証処理を実行（図１３参照）し、認証が成立したことを条件として（Ｓ２２０２の判定Ｙｅｓ）、相手の属性証明書の検証を属性証明書発行局の公開鍵を用いて実行（Ｓ２２０３）し、検証が成功し、公開鍵証明書とリンクする属性証明書を、公開鍵証明書および属性証明書に共通に格納された公開鍵証明書通し番号に基づいて確認した（Ｓ２２０４の判定Ｙｅｓ）ことを条件として、公開鍵証明書と同一の公開鍵証明書通し番号を格納した属性証明書から属性情報を取り出す（Ｓ２２０５）。属性情報が正当である場合に（Ｓ２２０６の判定Ｙｅｓ）、相互認証、属性確認が成功したものと判定（Ｓ２２０７）し、その後の処理に移行する。ステップＳ２２０２，Ｓ２２０４，Ｓ２２０６で判定がＮｏの場合は、相互認証、属性確認が失敗であると判定（Ｓ２２０８）され、その後の処理は中止される。

【０３７２】（２）トランザクションＩＤ、購入要求データ生成、および
（３）購入要求データ送信
上述のショップサーバ１０１０とユーザ機器１０２０間の相互認証および属性確認が成功すると、ユーザ機器１０２０は、コンテンツの購入要求データを生成する。購入要求データの構成は、先に説明した図１４（ａ）に示す構成であり、コンテンツ購入の要求先であるショップサーバ１０１０の識別子であるショップＩＤ、取り引きの識別子として、ユーザ機器１０２０の暗号処理手段が乱数に基づいて生成するトランザクションＩＤ、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツＩＤの各データを有し、これらのデータに対するユーザ機器の電子署名が付加されている。

【０３７３】（４）受信データ検証
図１４（ａ）に示す購入要求データをユーザ機器１０２０から受信したショップサーバは、受信データの検証処理を実行する。検証処理は、先に、図１５を用いて説明したように、ユーザ機器の公開鍵証明書Ｃｅｒｔ＿ＤＥＶの検証の後、公開鍵証明書からユーザ機器の公開鍵：ＫｐＤＥＶを取り出して、ユーザ機器の公開鍵：Ｋｐ＿ＤＥＶを用いて購入要求データのユーザ機器署名の検証を行なうものである。

【０３７４】検証がＯＫ、すなわち購入要求データの改竄がないと判定されると、受信データが正当なコンテンツ購入要求データであると判定される。検証が不成立の場合は、購入要求データが改竄ありと判定され、その購入要求データに対する処理が中止される。

【０３７５】（５）暗号化コンテンツおよび暗号化コンテンツ鍵データ１（ショップ）送信
ショップサーバ１０１０において、購入要求データの検証が完了し、データ改竄のない正当なコンテンツ購入要求であると判定すると、ショップサーバ１０１０は、暗号化コンテンツおよび暗号化コンテンツ鍵データ１（ショップ）をユーザ機器に送信する。これらは、いずれもコンテンツデータベースに格納されたデータであり、コンテンツをコンテンツキーで暗号化した暗号化コンテンツ：Ｋｃ（content）と、コンテンツキー：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）１０３０の公開鍵で暗号化した暗号化コンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）で

ある。

【０３７６】暗号化コンテンツ鍵データ１（ショップ）は、先に説明した図１４（ｂ）に示す構成である。すなわち、コンテンツ購入の要求元であるユーザ機器１０２０の識別子であるユーザ機器ＩＤ、購入要求データ（図１４（ａ）のユーザ機器公開鍵証明書を除いたデータ）、コンテンツ取り引きに伴いショップサーバ１０１０が生成したショップ処理Ｎｏ．、暗号化コンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）を有し、これらのデータに対するショップサーバ１０１０の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ１（ショップ）には、ショップサーバ１０１０の公開鍵証明書が添付され、ユーザ機器１０２０に送付される。なお、ショップサーバ公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ユーザ機器側に送付済みの場合は、必ずしも改めて送付する必要はない。

【０３７７】（６）受信データ検証

ショップサーバ１０１０から暗号化コンテンツ：Ｋｃ（content）と、図１４（ｂ）に示す暗号化コンテンツ鍵データ１（ショップ）を受信したユーザ機器１０２０は、暗号化コンテンツ鍵データ１（ショップ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器１０２０は、まずショップサーバ１０１０から受領したショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵ＫｐＳＨＯＰを用いて図１４（ｂ）に示す暗号化コンテンツ鍵データ１のショップ署名の検証を実行する。

【０３７８】（７）相互認証および属性確認処理

ユーザ機器１０２０が、ショップサーバ１０１０から暗号化コンテンツ：Ｋｃ（content）と暗号化コンテンツ鍵データ１（ショップ）を受信し、暗号化コンテンツ鍵データ１（ショップ）の検証を終えると、ユーザ機器１０２０は、ユーザ機器認証サーバ１０３０にアクセスし、ユーザ機器１０２０と、ユーザ機器認証サーバ１０３０間において相互認証処理および属性確認処理を実行する。この処理は、前述のショップサーバ１０１０とユーザ機器１０２０間の相互認証処理および属性確認処理と同様の手続きで実行される。

【０３７９】（８）暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求送信

ユーザ機器１０２０とユーザ機器認証サーバ１０３０との間の相互認証および属性確認が成立すると、ユーザ機器１０２０は、ユーザ機器認証サーバ１０３０に対して、先にショップサーバ１０１０から受信した暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）と、暗号化コンテンツ鍵かけかえ要求を送信する。暗号化コンテンツ鍵データ（ユーザ機器）の構成は、先に説明した図１４（ｃ）に示す構成である。すなわち、暗号化コンテンツ鍵かけかえ要求の要求先であるユーザ機器認証サーバ１０３０の識別子であるユーザ機器認証サーバＩＤ、ショップサーバ１０１０から受領した暗号化コンテンツ鍵データ（図１４（ｂ）のショップ公開鍵証明書を除いたデータ）、を有し、これらのデータに対するユーザ機器１０２０の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ（ユーザ機器）には、ショップサーバ１０１０の公開鍵証明書と、ユーザ機器１０２０の公開鍵証明書が添付され、ユーザ機器認証サーバ１０３０に送付される。なお、ユーザ機器認証サーバ１０３０がユーザ機器公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【０３８０】（９）受信データ検証

ユーザ機器１０２０から暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求（図１４（ｃ））を受信したユーザ機器認証サーバ１０３０は、暗号化コンテンツ鍵かけかえ要求の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器認証サーバ１０３０は、まずユーザ機器１０２０から受領したユーザ機器の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器の公開鍵ＫｐＤＥＶを用いて図１４（ｃ）に示す暗号化コンテンツ鍵データ（ユーザ機器）の電子署名の検証を実行する。さらに、ショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵ＫｐＳＨＯＰを用いて図１４（ｃ）に示す暗号化コンテンツ鍵データ（ユーザ機器）に含まれる（５）暗号化コンテンツ鍵データ１のショップ署名の検証を実行する。また、ユーザ機器の送信した電文が図１４（ｃ）に示すフォーマット中に入っている場合は、その電文の検証を必要に応じて実行する。

【０３８１】（１０）暗号化コンテンツ鍵かけかえ処理

ユーザ機器認証サーバ１０３０において、ユーザ機器１０２０から受信した暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求の検証が終了し、正当な鍵かけかえ要求であると判定すると、ユーザ機器認証サーバ１０３０は、暗号化コンテンツ鍵データ（ユーザ機器）に含まれる暗号化コンテンツ鍵、すなわち、コンテンツ鍵：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）１０３０の公開鍵ＫｐＤＡＳで暗号化したデータ：ＫｐＤＡＳ（Ｋｃ）をユーザ機器認証サーバ１０３０の秘密鍵ＫｓＤＡＳで復号してコンテンツ鍵Ｋｃを取得し、さらにコンテンツ鍵Ｋｃをユーザ機器の公開鍵：ＫｐＤＥＶで暗号化した暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を生成する。すなわち、ＫｐＤＡＳ（Ｋｃ）→Ｋｃ→ＫｐＤＥＶ（Ｋｃ）の鍵かけかえ処理を実行する。

【０３８２】この処理は先に図１６を用いて説明したように、暗号化コンテンツ鍵データ（ユーザ機器）から、ユーザ機器認証サーバ（ＤＡＳ）１０３０の公開鍵ＫｐＤＡＳで暗号化したコンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）を取り出し、次に、ユーザ機器認証サーバ１０３０の秘密鍵ＫｓＤＡＳで復号してコンテンツ鍵Ｋｃを取得し、次に、復号により取得したコンテンツ鍵Ｋｃをユーザ機器の公開鍵：ＫｐＤＥＶで再暗号化して暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を生成する処理である。

【０３８３】（１１）相互認証および属性確認処理

ユーザ機器認証サーバ１０３０において、上述の暗号化コンテンツ鍵の鍵かけかえ処理が完了すると、ユーザ機器認証サーバ１０３０は、ショップサーバ１０１０にアクセスし、ユーザ機器認証サーバ１０３０とショップサーバ１０１０間において相互認証処理および属性確認処理を実行する。この処理は、前述のショップサーバ１０１０とユーザ機器１０２０間の相互認証処理および属性確認処理と同様の手続きで実行される。

【０３８４】（１２）暗号化コンテンツデータ送信

ユーザ機器認証サーバ１０３０とショップサーバ１０１０間の相互認証および属性確認処理が成立すると、ユーザ機器認証サーバ１０３０は、暗号化コンテンツ鍵データ（ＤＡＳ）をショップサーバ１０１０に送信する。暗号化コンテンツ鍵データ（ＤＡＳ）の構成は、先に説明した図１７（ｄ）に示す構成である。コンテンツ購入の要求先であるショップサーバ１０１０の識別子であるショップＩＤ、暗号化コンテンツ鍵データ（ユーザ機器）（図１４（ｃ）のショップおよびユーザ機器公開鍵証明書を除いたデータ）、さらに、前述の鍵かけかえ処理により、ユーザ機器認証サーバ１０３０が生成した暗号化コンテンツ鍵データ：ＫｐＤＥＶ（Ｋｃ）を有し、これらのデータに対するユーザ機器認証サーバ１０３０の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ（ＤＡＳ）には、ユーザ機器認証サーバ１０３０と、ユーザ機器１０２０の公開鍵証明書が添付され、ショップサーバ１０１０に送付される。なお、ショップサーバが、これらの公開鍵証明書を既に保有済みである場合は、必ずしも改めて送付する必要はない。

【０３８５】また、ユーザ機器認証サーバ１０３０が信頼できる第三者機関であると認められる存在である場合は、暗号化コンテンツ鍵データ（ＤＡＳ）は、図１７（ｄ）に示すようにユーザ機器の生成した（８）暗号化コンテンツ鍵データ（ユーザ機器）をそのまま含むデータ構成とすることなく、図１８（ｄ’）に示すように、ユーザ機器ＩＤ、トランザクションＩＤ、コンテンツＩＤ、ショップ処理ＮＯ、ユーザデバイスの公開鍵で暗号化したコンテンツ鍵ＫｐＤＥＶ（Ｋｃ）の各データを、ユーザ機器認証サーバ１０３０が抽出して、これらに署名を付加して暗号化コンテンツ鍵データ（ＤＡＳ）としてもよい。この場合は、（８）暗号化コンテンツ鍵データ（ユーザ機器）の検証が不要となるので、添付する公開鍵証明書は、ユーザ機器認証サーバ１０３０の公開鍵証明書のみでよい。

【０３８６】（１３）受信データ検証

ユーザ機器認証サーバ１０３０から暗号化コンテンツ鍵データ（ＤＡＳ）（図１７（ｄ））を受信したショップサーバ１０１０は、暗号化コンテンツ鍵データ（ＤＡＳ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ショップサーバ１０１０は、まずユーザ機器認証サーバ１０３０から受領したユーザ機器認証サーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ１０３０の公開鍵ＫｐＤＡＳを用いて図１７（ｄ）に示す暗号化コンテンツ鍵データ（ＤＡＳ）の電子署名の検証を実行する。さらに、ユーザ機器の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器の公開鍵ＫｐＤＥＶを用いて図１７（ｄ）に示す暗号化コンテンツ鍵データ（ＤＡＳ）に含まれる（８）暗号化コンテンツ鍵データ（ユーザ機器）のユーザ機器署名の検証を実行する。また、ユーザ機器の送信した電文が図１４（ｃ）に示すフォーマット中に入っている場合は、その電文の検証を必要に応じて実行する。

【０３８７】なお、先に説明した図１８（ｄ’）の簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）をショップサーバ１０１０が受領した場合は、ショップサーバ１０１０は、ユーザ機器認証サーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ１０３０の公開鍵ＫｐＤＡＳを用いて図１８（ｄ’）に示す暗号化コンテンツ鍵データ（ＤＡＳ）の電子署名の検証を実行するのみの処理となる。

【０３８８】（１４）相互認証および属性確認

（１５）暗号化コンテンツ鍵要求データ送信

次に、ユーザ機器１０２０は、暗号化コンテンツ鍵要求データをショップサーバに対して送信する。なお、この際、前の要求と異なるセッションで要求を実行する場合は、再度相互認証および属性確認を実行して、相互認証および属性確認が成立したことを条件として暗号化コンテンツ鍵要求データがユーザ機器１０２０からショップサーバ１０１０に送信される。また、ユーザ機器の送信した電文が図１４（ｃ）に示すフォーマット中に入っている場合は、その電文の検証を必要に応じて実行する。

【０３８９】暗号化コンテンツ鍵要求データの構成は図１７（ｅ）に示す通りである。暗号化コンテンツ鍵要求データは、コンテンツ購入の要求先であるショップサーバ１０１０の識別子であるショップＩＤ、取り引きの識別子として、ユーザ機器１０２０の暗号処理手段が乱数

に基づいて生成するトランザクションＩＤ、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツＩＤ、さらに、先にショップが生成し暗号化コンテンツ鍵データ１（ショップ）としてユーザ機器１０２０に送信してきたデータ（図１４（ｂ）参照）中に含まれるショップ処理Ｎｏ．を有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、暗号化コンテンツ鍵要求データには、ユーザ機器の公開鍵証明書が添付され、ショップサーバ１０１０に送付される。なお、公開鍵証明書が既にショップ側に保管済みの場合は、必ずしも改めて送付する必要はない。

【０３９０】（１６）検証処理、および
（１７）課金処理

暗号化コンテンツ鍵要求データをユーザ機器から受信したショップサーバ１０１０は、暗号化コンテンツ鍵要求データの検証処理を実行する。これは、図１５を用いて説明したと同様の処理である。データ検証が済むと、ショップサーバ１０１０は、コンテンツの取り引きに関する課金処理を実行する。課金処理は、ユーザの取り引き口座からコンテンツ料金を受領する処理である。受領したコンテンツ料金は、コンテンツの著作権者、ショップ、ユーザ機器認証サーバ管理者など、様々な関係者に配分される。

【０３９１】この課金処理に至るまでには、ユーザ機器認証サーバ１０３０による暗号化コンテンツ鍵の鍵かけかえ処理プロセスが必須となっているので、ショップサーバ１０１０は、ユーザ機器間とのみの処理では課金処理が実行できない。また、ユーザ機器１０２０においても暗号化コンテンツ鍵の復号ができないので、コンテンツの利用ができない。ユーザ機器認証サーバは、図６を用いて説明したユーザ機器認証サーバ・ライセンス管理データベースに、すべての鍵かけかえ処理を実行したコンテンツ取り引き内容を記録しており、すべての課金対象となるコンテンツ取り引きが把握可能となる。従って、ショップ側単独でのコンテンツ取り引きは不可能となり、不正なコンテンツ販売が防止される。

【０３９２】（１８）暗号化コンテンツ鍵データ２（ショップ）送信

ショップサーバ１０１０における課金処理が終了すると、ショップサーバ１０１０は、暗号化コンテンツ鍵データ２（ショップ）をユーザ機器１０２０に送信する。

【０３９３】暗号化コンテンツ鍵データ２（ショップ）の構成は、先に説明した図１７（ｆ）に示す通りである。暗号化コンテンツ鍵要求の要求元であるユーザ機器１０２０の識別子であるユーザ機器ＩＤ、ユーザ機器認証サーバ１０３０から受領した暗号化コンテンツ鍵データ（ＤＡＳ）（図１７（ｄ）のユーザ機器、ユーザ機器認証サーバ公開鍵証明書を除いたデータ）、を有し、これらのデータに対するショップサーバ１０１０の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ２（ショップ）には、ショップサーバ１０１０の公開鍵証明書と、ユーザ機器認証サーバ１０３０の公開鍵証明書が添付され、ユーザ機器１０２０に送付される。なお、ユーザ機器１０２０がユーザ機器認証サーバ公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【０３９４】なお、ユーザ機器認証サーバ１０３０が信頼できる第三者機関であると認められる存在であり、ショップサーバ１０１０がユーザ機器認証サーバ１０３０から受信する暗号化コンテンツ鍵データ（ＤＡＳ）が先に説明した図１８（ｄ’）の簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）である場合は、ショップサーバ１０１０は、図１８（ｆ’）に示す暗号化コンテンツ鍵データ２（ショップ）をユーザ機器に送付する。すなわち、図１８（ｄ’）に示す簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）にショップサーバの署名を付加したデータに、ショップサーバ１０１０の公開鍵証明書と、ユーザ機器認証サーバ１０３０の公開鍵証明書が添付してユーザ機器１０２０に送付する。

【０３９５】（１９）受信データ検証

ショップサーバ１０１０から、暗号化コンテンツ鍵データ２（ショップ）を受領したユーザ機器１０２０は、暗号化コンテンツ鍵データ２（ショップ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器１０２０は、まずショップサーバ１０１０から受領したショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバ１０１０の公開鍵ＫｐＳＨＯＰを用いて図１７（ｆ）に示す暗号化コンテンツ鍵データ２（ショップ）の電子署名の検証を実行する。さらに、ユーザ機器認証サーバ１０３０の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ１０３０の公開鍵ＫｐＤＡＳを用いて図１７（ｆ）に示す暗号化コンテンツ鍵データ２（ショップ）に含まれる（１２）暗号化コンテンツ鍵データ（ＤＡＳ）の署名検証を実行する。また、何らかの送信電文が図１７（ｆ）に示すフォーマット中に入っている場合は、その電文の検証を必要に応じて実行する。

【０３９６】（２０）保存処理

ショップサーバ１０１０から受信した暗号化コンテンツ鍵データ２（ショップ）を検証したユーザ機器１０２０は、暗号化コンテンツ鍵データ２（ショップ）に含まれる自己の公開鍵ＫｐＤＥＶで暗号化された暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を自己の秘密鍵ＫｓＤＥＶを用いて復号し、さらに、ユーザ機器の保存鍵Ｋｓｔｏを用いて暗号化して暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を生成して、これをユーザ機器１０２０の記憶手段に格納する。コンテンツの利用時には、暗号化コンテン

ツ鍵：Ｋｓｔｏ（Ｋｃ）を保存鍵Ｋｓｔｏを用いて復号してコンテンツ鍵Ｋｃを取り出して、取り出したコンテンツ鍵Ｋｃを用いて、暗号化コンテンツＫｃ（Content）の復号処理を実行し、コンテンツ（Content）を再生、実行する。

【０３９７】以上、述べたように、コンテンツ配信に伴う各処理において、通信を実行する各エンティテイは、属性確認により、相手の属性、例えばユーザ機器であることを確認した後、処理を実行する構成としたので、不当なコンテンツ取り引き、例えばショップがユーザ機器になりすましてコンテンツを取り引きするなどの処理、あるいは、ショップサーバになりすまして、ユーザ機器からクレジット口座番号を不正に取得する等の処理が防止される。

【０３９８】例えばユーザ機器は、属性確認により、ユーザ機器の通信相手がショップであると確認されれば、ショップに対する処理としてのコンテンツ購入に伴う処理を安心して実行可能であり、また属性確認において、通信相手がユーザ機器認証サーバであると確認されれば、ユーザ機器認証サーバに対する処理、例えば鍵のかけかえ要求の送信を実行することができる。本構成によれば、属性確認を行なうことにより通信相手の属性が確認可能となるので、それぞれの通信相手に応じた正当な処理が実行される。さらに、不正な通信相手に秘密データを誤って送信することもなくなるので、データ漏洩の防止も可能である。

【０３９９】次に、相互認証処理による相手確認を実行せず、受信データの署名検証のみを実行して、データ改竄の有無と、属性確認を実行してコンテンツ取り引き処理を実行する形態について図７４を用いて説明する。

【０４００】図７４に示す処理は、図７２に示す処理から相互認証処理を省いた処理として実行されるものである。図７４の番号（１）から（１６）の順に処理が進行する。各番号順に処理の詳細を説明する。

【０４０１】（１）トランザクションＩＤ、購入要求データ生成、および

（２）購入要求データ送信

まず、ユーザ機器１０２０は、コンテンツの購入要求データを生成し、ショップサーバ１０１０に送信する。購入要求データの構成は、先に説明した図１４（ａ）に示す構成である。

【０４０２】（３）受信データ検証

図１４（ａ）に示す購入要求データをユーザ機器１０２０から受信したショップサーバは、受信データの検証処理を実行する。本実施例における検証処理は、購入要求データの改竄有無のチェックとともに、属性情報のチェックも併せて実行するものである。

【０４０３】図７５に公開鍵証明書に属性情報が格納されている場合の受信データ検証処理フローを示す。まず、メッセージと署名（購入要求データ）と、ユーザ機器の公開鍵証明書を受信（Ｓ２３０１）したショップサーバ１０１０は、ユーザ機器の公開鍵証明書を公開鍵証明書発行局の公開鍵ＫｐＣＡを用いて検証（Ｓ２３０２）する。検証が成立（Ｓ２３０３でＹｅｓ）すると、公開鍵証明書からユーザ機器の公開鍵：ＫｐＤＥＶを取り出し（Ｓ２３０４）て、ユーザ機器の公開鍵：ＫｐＤＥＶを用いて購入要求データのユーザ機器署名の検証（Ｓ２３０５）を行なう。さらに、検証が成功（Ｓ２３０６でＹｅｓ）すると、公開鍵証明書から属性情報を取り出し（Ｓ２３０７）て、正当な属性（ここではユーザ機器を示す属性）であるか否かを判定（Ｓ２３０８）し、正当である場合は、検証処理成功（Ｓ２３０９）として、次の処理に移行する。ステップＳ２３０３，Ｓ２３０６，Ｓ２３０８で判定がＮｏの場合は、検証処理失敗（Ｓ２３１０）として処理を中止する。

【０４０４】次に、公開鍵証明書と属性証明書を用いた受信データ検証処理について図７６のフローを用いて説明する。まず、メッセージと署名（購入要求データ）と、ユーザ機器の公開鍵証明書、属性証明書を受信（Ｓ２４０１）したショップサーバ１０１０は、ユーザ機器の公開鍵証明書を公開鍵証明書発行局の公開鍵ＫｐＣＡを用いて検証（Ｓ２４０２）する。検証が成立（Ｓ２４０３でＹｅｓ）すると、公開鍵証明書からユーザ機器の公開鍵：ＫｐＤＥＶを取り出し（Ｓ２４０４）て、ユーザ機器の公開鍵：ＫｐＤＥＶを用いて購入要求データのユーザ機器署名の検証（Ｓ２４０５）を行なう。さらに、検証が成功（Ｓ２４０６でＹｅｓ）すると、属性証明書を属性証明書発行局の公開鍵ＫｐＡＡを用いて検証（Ｓ２４０７）する。検証が成功（Ｓ２４０８でＹｅｓ）したことを条件として、属性証明書から属性情報を取り出し（Ｓ２４０９）て、正当な属性（ここではユーザ機器を示す属性）であるか否かを判定（Ｓ２４１０）し、正当である場合は、検証処理成功（Ｓ２４１１）として、次の処理に移行する。ステップＳ２４０３，Ｓ２４０６，Ｓ２４０８，Ｓ２４１０で判定がＮｏの場合は、検証処理失敗（Ｓ２４１２）として処理を中止する。

【０４０５】（４）暗号化コンテンツおよび暗号化コンテンツ鍵データ１（ショップ）送信

ショップサーバ１０１０において、購入要求データの検証が完了し、データ改竄のない正当なコンテンツ購入要求であると判定され属性が確認されると、ショップサーバ１０１０は、暗号化コンテンツおよび暗号化コンテンツ鍵データ１（ショップ）（図１４（ｂ）参照）をユーザ機器に送信する。

【０４０６】（５）受信データ検証

ショップサーバ１０１０から暗号化コンテンツ：Ｋｃ（content）と、図１４（ｂ）に示す暗号化コンテンツ鍵データ１（ショップ）を受信したユーザ機器１０２０は、暗号化コンテンツ鍵データ１（ショップ）の検証処

理および属性確認処理を実行する。この検証処理は、先に説明した図７５または図７６の処理フローと同様の処理である。この場合、公開鍵証明書または属性証明書の属性がショップを示していない場合は、処理が中止されることになる。

【０４０７】（６）暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求送信

次に、ユーザ機器１０２０は、ユーザ機器認証サーバ１０３０に対して、先にショップサーバ１０１０から受信した暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）と、暗号化コンテンツ鍵かけかえ要求（図１４（ｃ）参照）を送信する。

【０４０８】（７）受信データ検証

ユーザ機器１０２０から暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求（図１４（ｃ））を受信したユーザ機器認証サーバ１０３０は、暗号化コンテンツ鍵かけかえ要求の検証処理を実行する。この検証処理は、先に説明した図７５、図７６の処理フローと同様の処理であり、属性確認も併せて実行する処理である。この場合は公開鍵証明書または属性証明書の属性がユーザ機器でない場合は、処理が中止される。

【０４０９】（８）暗号化コンテンツ鍵かけかえ処理、

次に、ユーザ機器認証サーバ１０３０において、ＫｐＤＡＳ（Ｋｃ）→Ｋｃ→ＫｐＤＥＶ（Ｋｃ）の鍵かけかえ処理を実行する。

【０４１０】（９）暗号化コンテンツデータ送信

次に、ユーザ機器認証サーバ１０３０は、暗号化コンテンツ鍵データ（ＤＡＳ）をショップサーバ１０１０に送信する。暗号化コンテンツ鍵データ（ＤＡＳ）の構成は、先に説明した図１７（ｄ）に示す構成である。

【０４１１】（１０）受信データ検証

ユーザ機器認証サーバ１０３０から暗号化コンテンツ鍵データ（ＤＡＳ）（図１７（ｄ））を受信したショップサーバ１０１０は、暗号化コンテンツ鍵データ（ＤＡＳ）の検証処理を実行する。この検証処理は、先に説明した図７５、図７６の処理フローと同様の処理であり、属性確認が併せて実行される。この場合は公開鍵証明書または属性証明書の属性がユーザ機器認証サーバ（サービス運営体）でない場合は、処理が中止される。

【０４１２】（１１）暗号化コンテンツ鍵要求データ送信

次に、ユーザ機器１０２０は、暗号化コンテンツ鍵要求データをショップサーバに対して送信する。暗号化コンテンツ鍵要求データの構成は図１７（ｅ）に示す通りである。

【０４１３】（１２）検証処理、および

（１３）課金処理

暗号化コンテンツ鍵要求データをユーザ機器から受信したショップサーバ１０１０は、暗号化コンテンツ鍵要求データの検証処理を実行する。これは、先に説明した図７５、図７６の処理フローと同様の処理であり、属性確認も併せて実行する処理である。この場合は公開鍵証明書または属性証明書の属性がユーザ機器でない場合は、処理が中止される。データ検証が済むと、ショップサーバ１０１０は、コンテンツの取り引きに関する課金処理を実行する。

【０４１４】（１４）暗号化コンテンツ鍵データ２（ショップ）送信

ショップサーバ１０１０における課金処理が終了すると、ショップサーバ１０１０は、暗号化コンテンツ鍵データ２（ショップ）をユーザ機器１０２０に送信する。暗号化コンテンツ鍵データ２（ショップ）の構成は、先に説明した図１７（ｆ）に示す通りである。

【０４１５】（１５）受信データ検証

（１６）保存処理

ショップサーバ１０１０から、暗号化コンテンツ鍵データ２（ショップ）を受領したユーザ機器１０２０は、暗号化コンテンツ鍵データ２（ショップ）の検証処理を実行する。この検証処理は、先に説明した図７５、図７６の処理フローと同様の処理であり、属性確認も併せて実行する処理である。この場合は公開鍵証明書または属性証明書の属性がショップでない場合は、処理が中止される。データ検証が済むと、ユーザ機器１０２０は、コンテンツの保存処理、すなわち自己の公開鍵ＫｐＤＥＶで暗号化された暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を自己の秘密鍵ＫｓＤＥＶを用いて復号し、さらに、ユーザ機器の保存鍵Ｋｓｔｏを用いて暗号化して暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を生成して、これをユーザ機器１０２０の記憶手段に格納する処理を実行する。

【０４１６】このように、図７４に示す処理においては、相互認証時に属性確認を行なうのではなく、受信したデータの署名検証において、属性を確認する処理を実行する構成としたので、処理が簡略化され、コンテンツ取り引きに伴う処理の効率化が達成される。

【０４１７】なお、上述した属性データによる属性確認を適用した実施例では、サービス運営体において、鍵かけかえ処理を実行する構成について説明したが、例えば前述のログ収集サーバを適用した構成においても属性確認処理を適用することが可能である。その他一般的なデータ送受信を実行するエンティティ間において、それぞれのエンティティに特徴づけられた機能に基づいて属性を設定し、設定された属性を公開鍵証明書または属性証明書に格納し、これらの証明書を用いて通信相手の属性確認処理を実行することにより、さらにデータ通信の安全性、セキュリティを高めることが可能となる。また、属性確認処理は、従来の相互認証処理、署名検証処理と併せて実行することが可能であるので、通常のデータ通信は、署名検証のみ、あるいは相互認証のみを行ない、必要に応じて属性確認処理を行なうなど、セキュリティ

度合いに応じて選択的に署名検証処理、相互認証処理、属性確認処理のいずれか、あるいは組み合わせて実行することが可能である。

【０４１８】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０４１９】

【発明の効果】上述したように、本発明のコンテンツ配信システムおよびコンテンツ配信方法によれば、コンテンツの購入要求を受け付けるショップサーバが、ユーザ機器のコンテンツ購入要求に対する課金処理が終了したことを条件として、ユーザ機器の格納鍵での復号可能な態様とした暗号化コンテンツ鍵をユーザ機器に送付する構成としたので、コンテンツの購入に伴う確実な課金処理が可能となる。

【０４２０】さらに、本発明のコンテンツ配信システムおよびコンテンツ配信方法によれば、ユーザ機器からのコンテンツ購入要求に基づいて、ユーザ機器認証サーバ（ＤＡＳ）の公開鍵で暗号化したコンテンツ鍵ＫｐＤＡＳ（Ｋｃ）をユーザ機器の公開鍵ＫｐＤＥＶで暗号化したコンテンツ鍵ＫｐＤＥＶ（Ｋｃ）にかけかえる処理をコンテンツ配信を管理するユーザ機器認証サーバが実行する構成としたので、ショップとユーザ機器間のコンテンツ取り引きをユーザ機器認証サーバが確実に把握することが可能となる。

【０４２１】さらに、本発明のコンテンツ配信システムおよびコンテンツ配信方法によれば、ユーザ機器、ショップ、ユーザ機器認証サーバ間で実行されるデータ通信では、相互認証処理あるいは署名生成、検証処理の少なくともいずれかを実行する構成としたので、データ通信のセキュリテイ、データ改竄のチェックが可能となる。

【図面の簡単な説明】

【図１】本発明のコンテンツ配信システムのシステム概要およびコンテンツ配信処理を説明する図である。

【図２】本発明のコンテンツ配信システムにおけるショップサーバの構成を示す図である。

【図３】本発明のコンテンツ配信システムにおけるショップサーバの購買管理データベースの構成を示す図である。

【図４】本発明のコンテンツ配信システムにおけるショップサーバの制御手段構成を示す図である。

【図５】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバの構成を示す図である。

【図６】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバのライセンス管理データベースの構成を示す図である。

【図７】本発明のコンテンツ配信システムにおけるユーザ機器の構成を示す図である。

【図８】本発明のコンテンツ配信システムにおけるユーザ機器の購入管理データベース構成を示す図である。

【図９】本発明のコンテンツ配信システムにおける公開鍵証明書配布構成を示す図である。

【図１０】本発明のコンテンツ配信システムにおいて適用可能な署名生成処理を説明する図である。

【図１１】本発明のコンテンツ配信システムにおいて適用可能な署名検証処理を説明する図である。

【図１２】本発明のコンテンツ配信システムにおいて適用可能な相互認証（対称鍵方式）処理を説明する図である。

【図１３】本発明のコンテンツ配信システムにおいて適用可能な相互認証（非対称鍵方式）処理を説明する図である。

【図１４】本発明のコンテンツ配信システムにおいて各エンティテイ間で通信されるデータ構成を説明する図である。

【図１５】本発明のコンテンツ配信システムにおいて適用可能なデータ検証処理を説明する図である。

【図１６】本発明のコンテンツ配信システムにおいて実行される鍵かけかえ処理を説明する図である。

【図１７】本発明のコンテンツ配信システムにおいて各エンティテイ間で通信されるデータ構成を説明する図である。

【図１８】本発明のコンテンツ配信システムにおいて各エンティテイ間で通信されるデータ構成を説明する図である。

【図１９】本発明のコンテンツ配信システムにおいて実行されるコンテンツ鍵保存処理を説明する図である。

【図２０】本発明のコンテンツ配信システムにおけるショップサーバのステータス変遷を説明する図である。

【図２１】本発明のコンテンツ配信システムにおけるユーザ機器のステータス変遷を説明する図である。

【図２２】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバのステータス変遷を説明する図である。

【図２３】本発明のコンテンツ配信システムにおけるショップサーバとユーザ機器間の処理フロー（その１）を示す図である。

【図２４】本発明のコンテンツ配信システムにおけるショップサーバとユーザ機器間の処理フロー（その２）を示す図である。

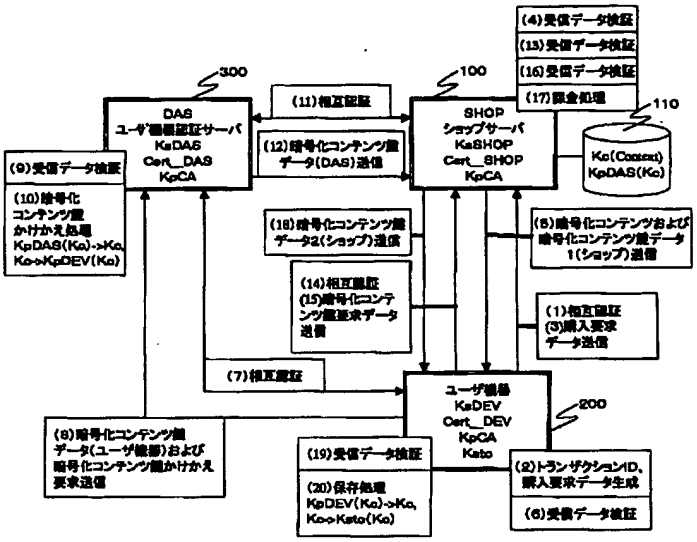
【図２５】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバとユーザ機器間の処理フローを示す図である。

【図２６】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバとショップサーバ間の処理フローを示す図である。

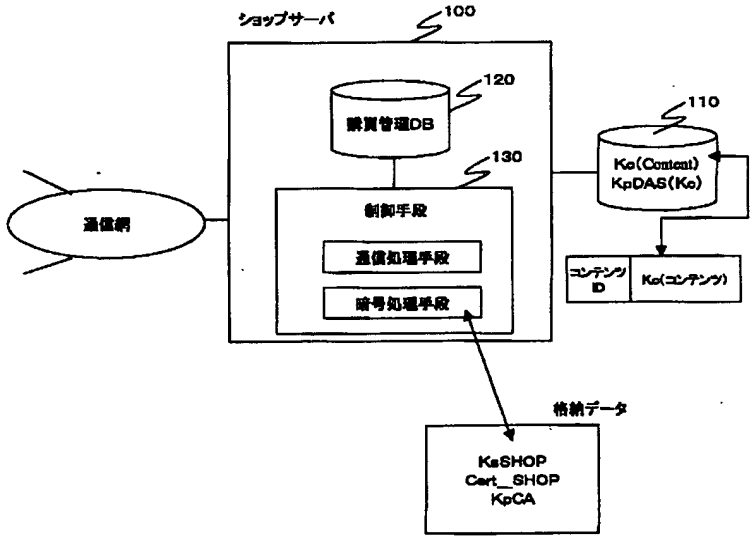
【図２７】本発明のコンテンツ配信システムにおけるショップサーバとユーザ機器間の処理フロー（その１）を示す図である。
【図２８】本発明のコンテンツ配信システムにおけるショップサーバとユーザ機器間の処理フロー（その２）を示す図である。
【図２９】本発明のコンテンツ配信システムの変形例として配信サーバを用いたコンテンツ配信処理を説明する図である。
【図３０】本発明のコンテンツ配信システムの変形例として配信サーバを用いたコンテンツ配信処理を説明する図である。
【図３１】本発明のコンテンツ配信システムの変形例のコンテンツ配信処理を説明する図である。
【図３２】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。
【図３３】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。
【図３４】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。
【図３５】本発明のコンテンツ配信システムの相互認証を伴わないコンテンツ配信処理を説明する図である。
【図３６】本発明のコンテンツ配信システムの相互認証を伴わないコンテンツ配信処理の変形例を説明する図である。
【図３７】本発明のコンテンツ配信システムにおいて電子チケットを適用したコンテンツ配信処理を説明する図である。
【図３８】本発明のコンテンツ配信システムのチケット発行サーバの構成を説明する図である。
【図３９】本発明のコンテンツ配信システムのチケット発行サーバのチケット発行管理データベース構成を説明する図である。
【図４０】本発明のコンテンツ配信システムのユーザ機器の購入管理データベース構成を説明する図である。
【図４１】本発明のコンテンツ配信システムのユーザ機器認証サーバのライセンス管理データベース構成を説明する図である。
【図４２】本発明のコンテンツ配信システムの配信サーバの構成を説明する図である。
【図４３】本発明のコンテンツ配信システムの配信サーバの配信管理データベース構成を説明する図である。
【図４４】本発明のコンテンツ配信システムのチケット換金サーバの構成を説明する図である。
【図４５】本発明のコンテンツ配信システムのチケット換金サーバのチケット換金管理データベース構成を説明する図である。
【図４６】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。
【図４７】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。
【図４８】本発明のコンテンツ配信システムにおけるチケット発行サーバのステータス変遷を説明する図である。
【図４９】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバのステータス変遷を説明する図である。
【図５０】本発明のコンテンツ配信システムにおける配信サーバのステータス変遷を説明する図である。
【図５１】本発明のコンテンツ配信システムにおけるユーザ機器のステータス変遷を説明する図である。
【図５２】本発明のコンテンツ配信システムにおけるチケット換金サーバのステータス変遷を説明する図である。
【図５３】本発明のコンテンツ配信システムにおいて電子チケットを適用したコンテンツ配信処理の具体例を説明する図である。
【図５４】本発明のコンテンツ配信システムにおいてログ収集サーバを適用したコンテンツ配信処理を説明する図である。
【図５５】本発明のコンテンツ配信システムにおける購入ログの構成例を説明する図である。
【図５６】本発明のコンテンツ配信システムにおけるログ収集サーバの構成を示す図である。
【図５７】本発明のコンテンツ配信システムにおけるユーザ機器と、ショップサーバ間の処理を示すフロー図（その１）である。
【図５８】本発明のコンテンツ配信システムにおけるユーザ機器と、ショップサーバ間の処理を示すフロー図（その２）である。
【図５９】本発明のコンテンツ配信システムにおける購入要求データと販売確認データのフォーマット例を示す図である。
【図６０】本発明のコンテンツ配信システムにおいてて着ようか能な改竄チェック値（ＩＣＶ）生成処理構成を示す図である。
【図６１】本発明のコンテンツ配信システムにおけるユーザ機器と、ログ収集サーバ間の処理を示すフロー図（その１）である。
【図６２】本発明のコンテンツ配信システムにおけるユーザ機器と、ログ収集サーバ間の処理を示すフロー図（その２）である。
【図６３】本発明のコンテンツ配信システムにおけるコンテンツプロバイダと、ログ収集サーバ間の処理を示すフロー図である。

【図６４】本発明のコンテンツ配信システムにおけるショップサーバと、ログ収集サーバ間の処理を示すフロー図である。
【図６５】本発明のコンテンツ配信システムにおけるショップサーバと、ログ収集サーバ間の処理を示すフロー図である。
【図６６】本発明のコンテンツ配信システムにおいて適用される属性情報について説明する図である。
【図６７】本発明のコンテンツ配信システムにおいて適用可能な属性情報を持つ公開鍵証明書構成を示す図である。
【図６８】本発明のコンテンツ配信システムにおいて適用可能な公開鍵証明書および属性証明書構成を示す図である。
【図６９】本発明のコンテンツ配信システムにおける公開鍵証明書の新規発行処理を説明する図である。
【図７０】本発明のコンテンツ配信システムにおける公開鍵証明書の更新処理を説明する図である。
【図７１】本発明のコンテンツ配信システムにおける属性証明書の新規発行処理を説明する図である。
【図７２】本発明のコンテンツ配信システムにおける属性チェックを伴うコンテンツ配信処理を説明する図である。
【図７３】本発明のコンテンツ配信システムにおける属性チェックを伴う相互認証処理を説明するフロー図である。
【図７４】本発明のコンテンツ配信システムにおける属性チェックを伴うコンテンツ配信処理を説明する図である。
【図７５】本発明のコンテンツ配信システムにおける属性チェックを伴うデータ検証処理を説明するフロー図である。
【図７６】本発明のコンテンツ配信システムにおける属性チェックを伴うデータ検証処理を説明するフロー図である。
【符号の説明】
１００　ショップサーバ
１１０　コンテンツデータベース
１２０　購買管理データベース
１３０　制御手段
１３１　制御部
１３２　ＲＯＭ
１３３　ＲＡＭ
１３４　表示部
１３５　入力部
１３６　ＨＤＤ
１３７　ドライブ
１３８　ネットワークインタフェース
２００　ユーザ機器
２２０　購入管理データベース
２３０　制御手段
３００　ユーザ機器認証サーバ
３２０　ライセンス管理データベース
３３０　制御手段
４００　配信サーバ
４１０　コンテンツデータベース
６１０　チケット発行サーバ
６１２　購買管理データベース
６１３　制御手段
６２０　ユーザ機器
６３０　ユーザ機器認証サーバ
６４０　配信サーバ
６４２　配信管理データベース
６４３　制御手段
６４４　コンテンツデータベース
６５０　チケット換金サーバ
６５２　チケット換金管理データベース
６５３　制御手段
８０１　チケット発行体
８０２　ユーザ機器
８０３　ライセンスホルダ
８０４　コンテンツ制作者
８０５　銀行
９０１　ショップサーバ
９０２　ユーザ機器
９０３　ログ収集サーバ
９０４　オーサリングサーバ
９０５　コンテンツプロバイダ
９０３１　ログ管理データベース
９０３２　制御手段
１０１０　ショップサーバ
１０２０　ユーザ機器
１０３０　サービス運営体
１０４０　公開鍵証明書発行局
１０５０　属性証明書発行局

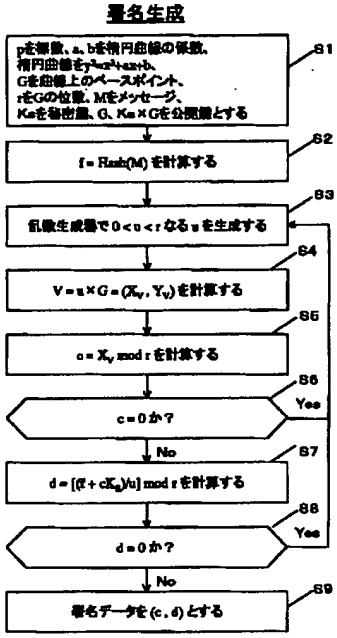
【図１】



【図２】



【図１０】



署名生成(IEEE P1363/D13)

【図６】

ユーザ機器認証サーバ処理No.	機器ID	トランザクションID	コンテンツID	ショップID	ショップ処理No.	ステータス
50001	1234567890	999888777	5000	1234	10001	鍵送信完了
50002	2345678901	666555444	4050	1234	10002	鍵かけかえ完了

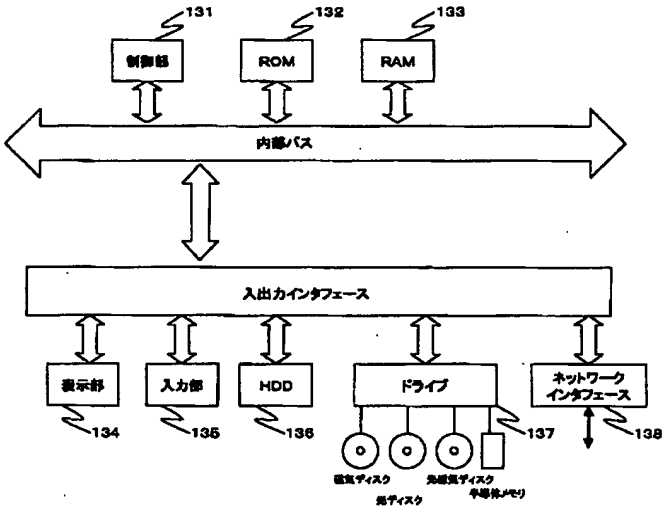
ユーザ機器認証サーバ・ライセンス管理DB

【図３】

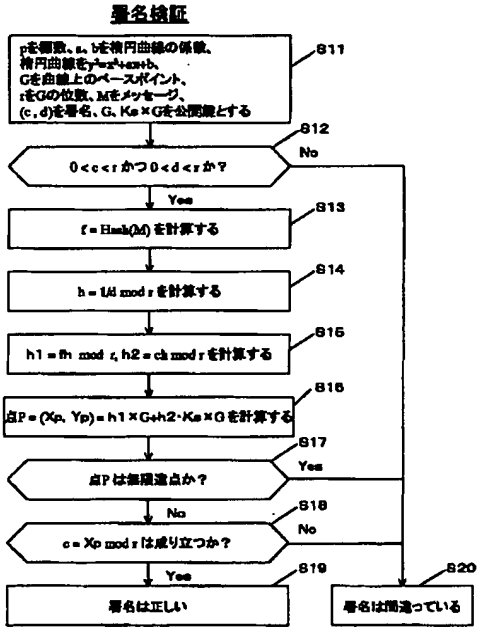
ショップ処理No.	機器ID	トランザクションID	コンテンツID	ステータス
10001	1234567890	999888777	5000	鍵2配信完了
10002	2345678901	666555444	4050	課金完了
10003	3456789012	333222111	1000	暗号化コンテンツ鍵送信要求受付完了
10004	4567890123	000999888	3000	鍵受信完了
10005	5678901234	777666555	5050	鍵1配信完了
10006	6789012345	444333222	2050	購入受付完了

ショップサーバ・購買管理DB

【図４】



【図１１】



署名検証(IEEE P1363/D13)

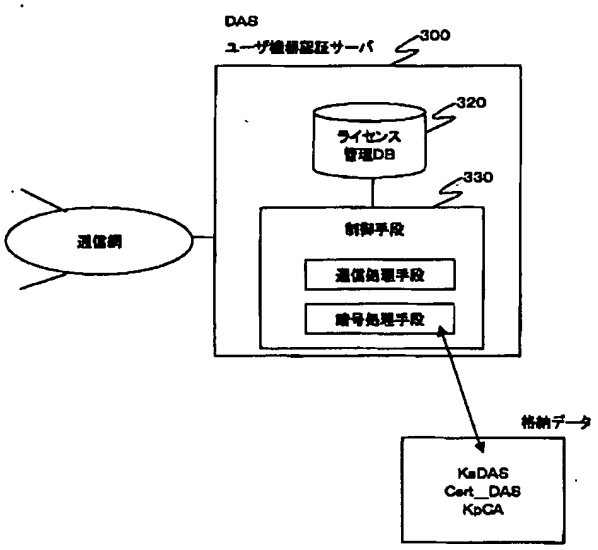
【図８】

機器ID:1234567890

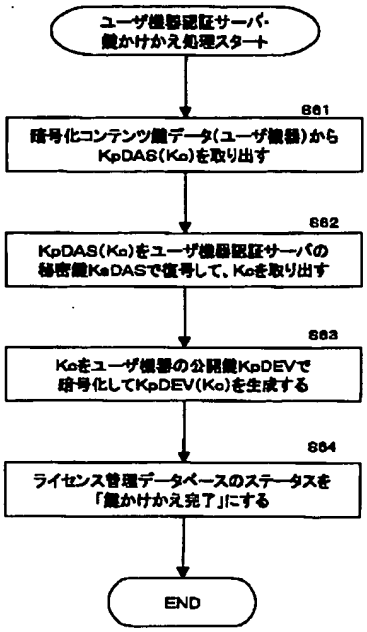
トランザクションID	コンテンツID	ショップID	ステータス
999888777	5000	1234	鍵2受信完了
666555444	4050	9876	購入要求送信完了

ユーザ機器・購入管理DB

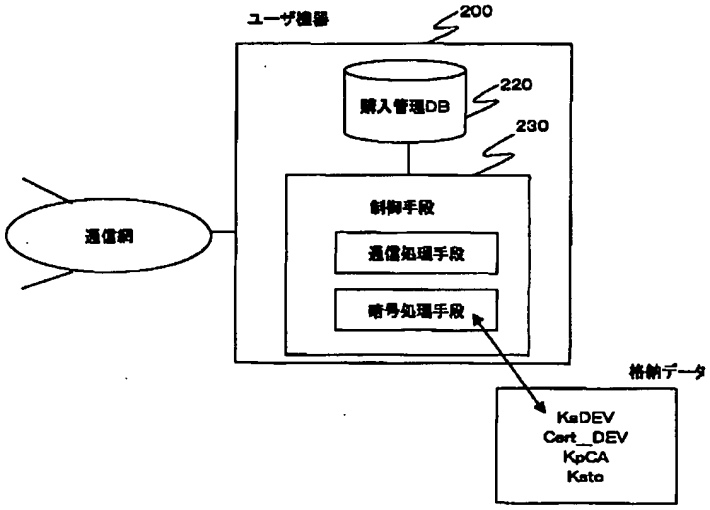
【図５】


DAS
ユーザ機器認証サーバ
300
320
ライセンス
管理DB
330
制御手段
通信処理手段
暗号処理手段
通信網
格納データ
KsDAS
Cert_DAS
KpCA

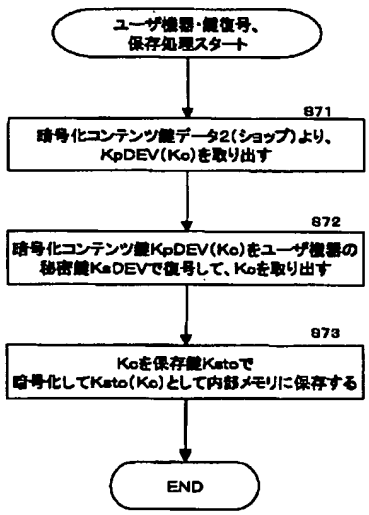
【図１６】


ユーザ機器認証サーバ・
鍵かけかえ処理スタート
S61
暗号化コンテンツ鍵データ(ユーザ機器)から
KpDAS(Ko)を取り出す
S62
KpDAS(Ko)をユーザ機器認証サーバの
秘密鍵KsDASで復号して、Koを取り出す
S63
Koをユーザ機器の公開鍵KpDEVで
暗号化してKpDEV(Ko)を生成する
S64
ライセンス管理データベースのステータスを
「鍵かけかえ完了」にする
END

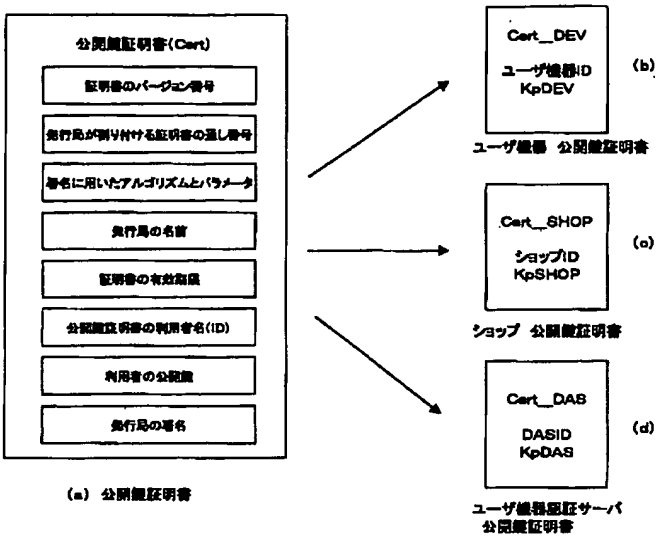
【図７】


ユーザ機器
200
220
購入管理DB
230
制御手段
通信処理手段
暗号処理手段
通信網
格納データ
KsDEV
Cert_DEV
KpCA
Ksto

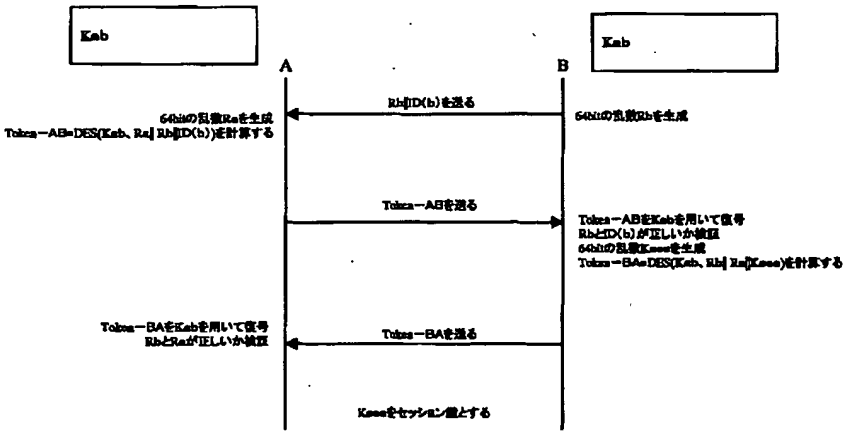
【図１９】


ユーザ機器・鍵復号、
保存処理スタート
S71
暗号化コンテンツ鍵データ2(ショップ)より、
KpDEV(Ko)を取り出す
S72
暗号化コンテンツ鍵KpDEV(Ko)をユーザ機器の
秘密鍵KsDEVで復号して、Koを取り出す
S73
Koを保存鍵Kstoで
暗号化してKsto(Ko)として内部メモリに保存する
END

【図９】

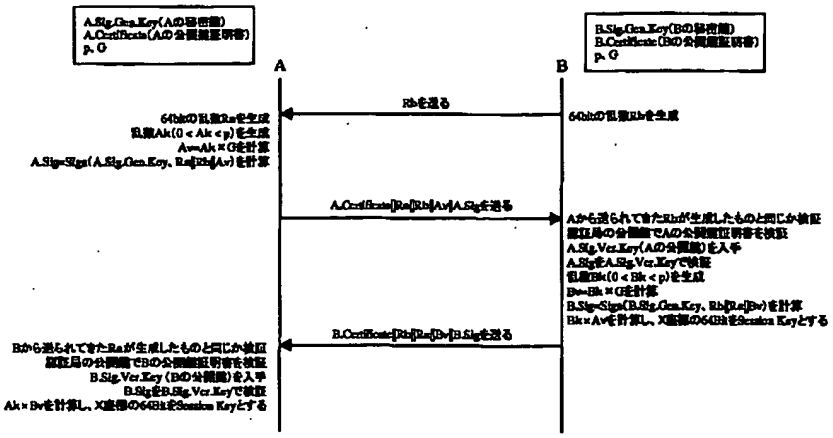


【図１２】



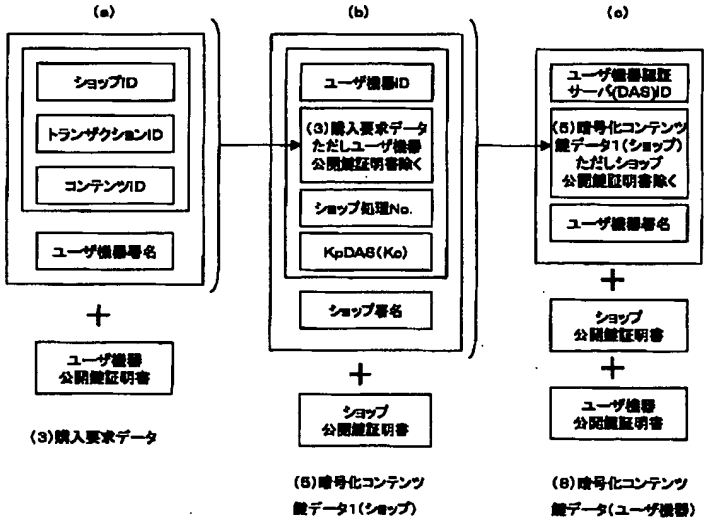
ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

【図１３】

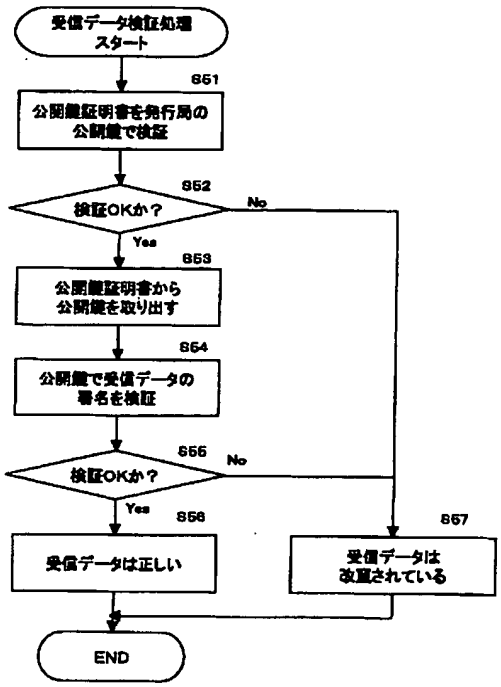


ISO/IEC 9798-3 非対称鍵暗号技術を用いた相互認証および鍵共有方式

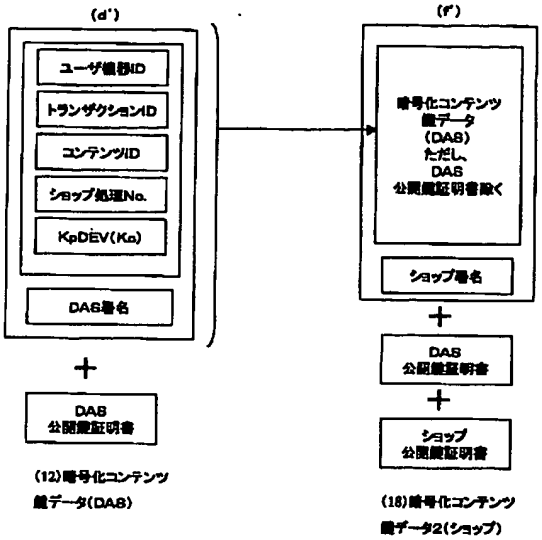
【図１４】



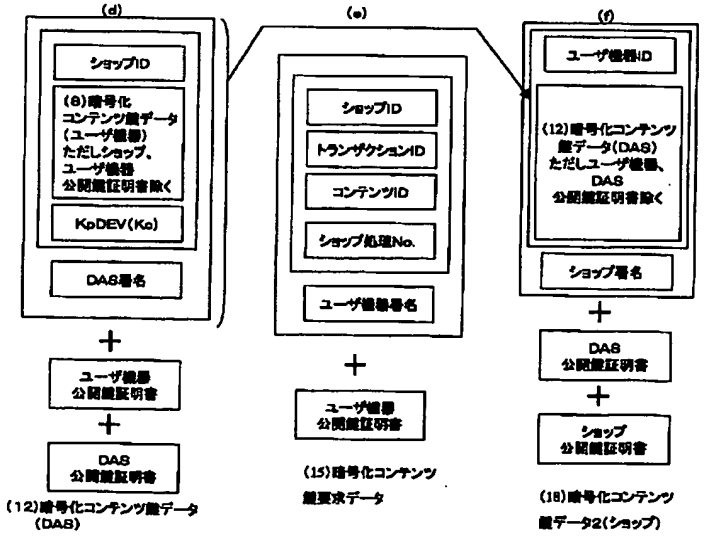
【図１５】


受信データ検証処理
スタート
S51
公開鍵証明書を発行局の
公開鍵で検証
S52
検証OKか？
No
Yes
S53
公開鍵証明書から
公開鍵を取り出す
S54
公開鍵で受信データの
署名を検証
S55
検証OKか？
No
Yes
S56
受信データは正しい
S57
受信データは
改竄されている
END

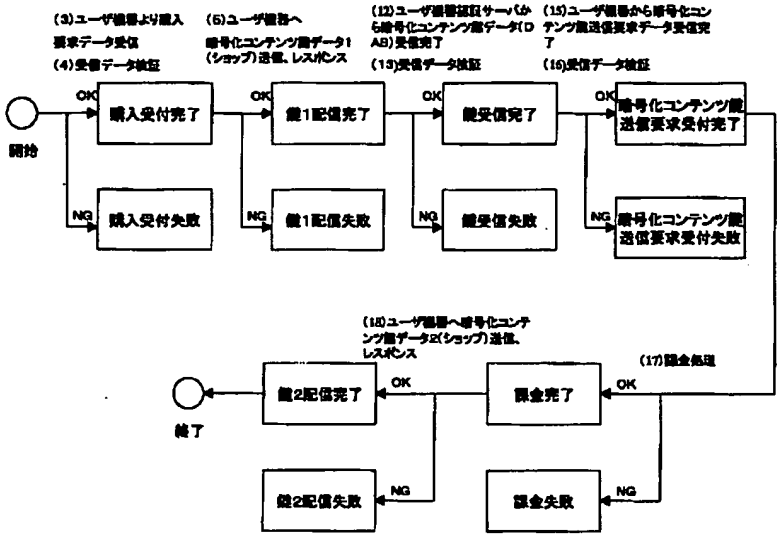
【図１８】


(d')
ユーザ機器ID
トランザクションID
コンテンツID
ショップ処理No.
KpDEV(Kc)
DAS署名
DAS
公開鍵証明書
(12)暗号化コンテンツ
鍵データ(DAS)
(f')
暗号化コンテンツ
鍵データ
(DAS)
ただし、
DAS
公開鍵証明書除く
ショップ署名
DAS
公開鍵証明書
ショップ
公開鍵証明書
(18)暗号化コンテンツ
鍵データ2(ショップ)

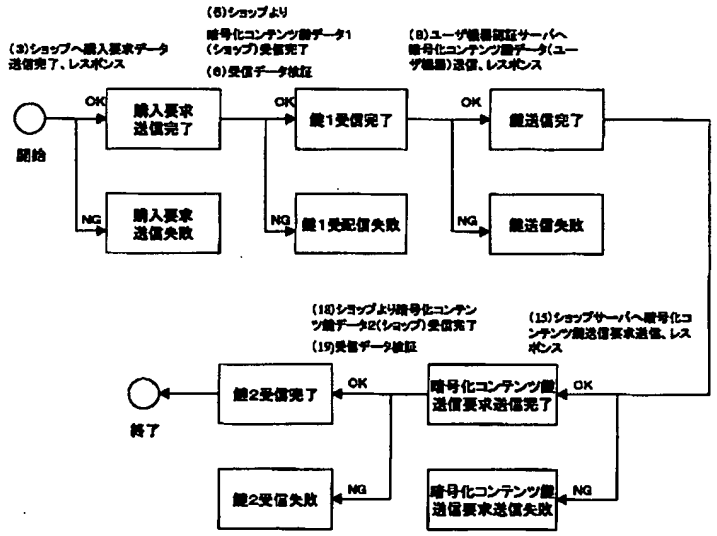
【図１７】


(d)
ショップID
(8)暗号化
コンテンツ鍵データ
(ユーザ機器)
ただしショップ、
ユーザ機器
公開鍵証明書除く
KpDEV(Kc)
DAS署名
ユーザ機器
公開鍵証明書
DAS
公開鍵証明書
(12)暗号化コンテンツ鍵データ
(DAS)
(e)
ショップID
トランザクションID
コンテンツID
ショップ処理No.
ユーザ機器署名
ユーザ機器
公開鍵証明書
(15)暗号化コンテンツ
鍵要求データ
(f)
ユーザ機器ID
(12)暗号化コンテンツ
鍵データ(DAS)
ただしユーザ機器、
DAS
公開鍵証明書除く
ショップ署名
DAS
公開鍵証明書
ショップ
公開鍵証明書
(18)暗号化コンテンツ
鍵データ2(ショップ)

【図２０】



【図２１】

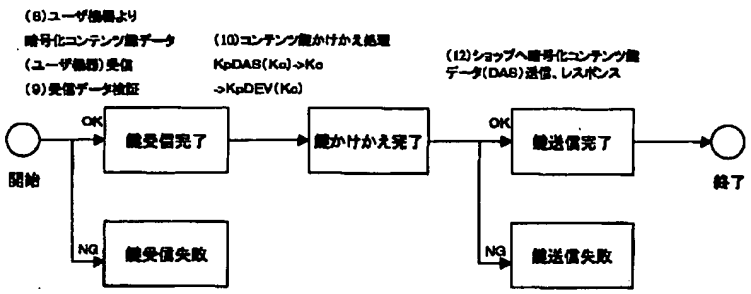


【図３９】

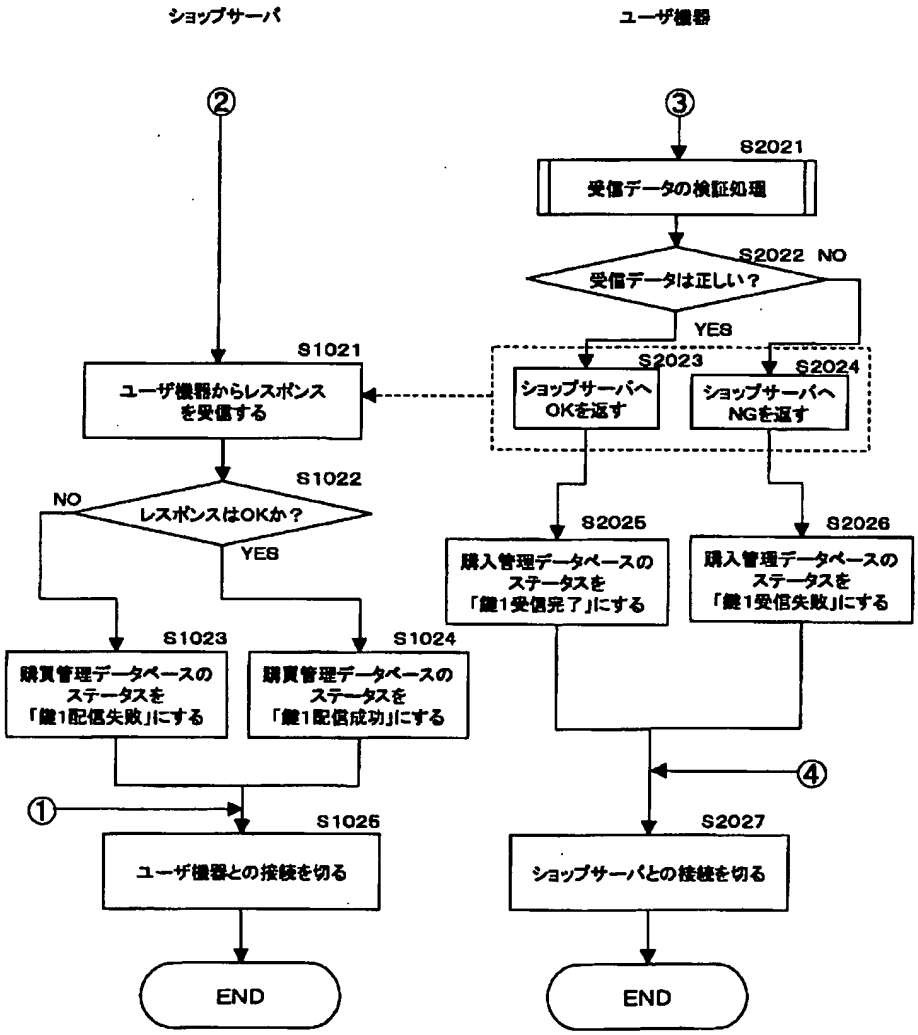
チケット発行処理No.	機器ID	トランザクションID	コンテンツID	チケット利用先ID	金額	有効期限	ステータス
10001	1234567890	999888777	5000	222331234	¥1000	00/04/01	決金処理レポート受信完了
10002	2345678901	666555444	4050	223345634	¥250	00/07/31	電子チケット配信完了
10003	3456788901	321655444	4021	345645234	¥800	00/07/31	購入受付完了

チケット発行サーバ・チケット発行管理DB

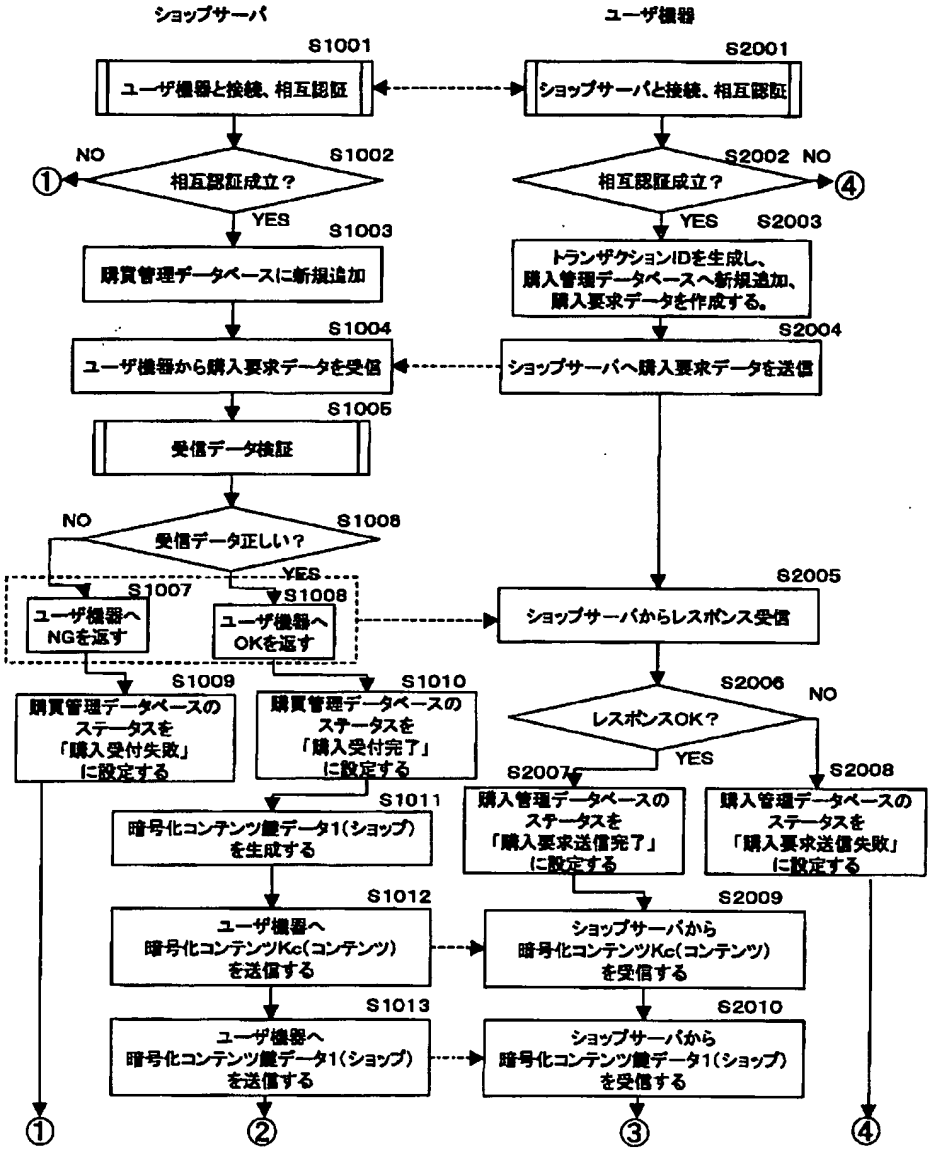
【図２２】


(8)ユーザ機器より
暗号化コンテンツ鍵データ
(ユーザ機器)受信
(9)受信データ検証
(10)コンテンツ鍵かけかえ処理
KpDAS(Ko)->Ko
->KpDEV(Ko)
(12)ショップへ暗号化コンテンツ鍵
データ(DAS)送信、レスポンス
開始
OK
鍵受信完了
鍵かけかえ完了
OK
鍵送信完了
終了
NG
鍵受信失敗
NG
鍵送信失敗

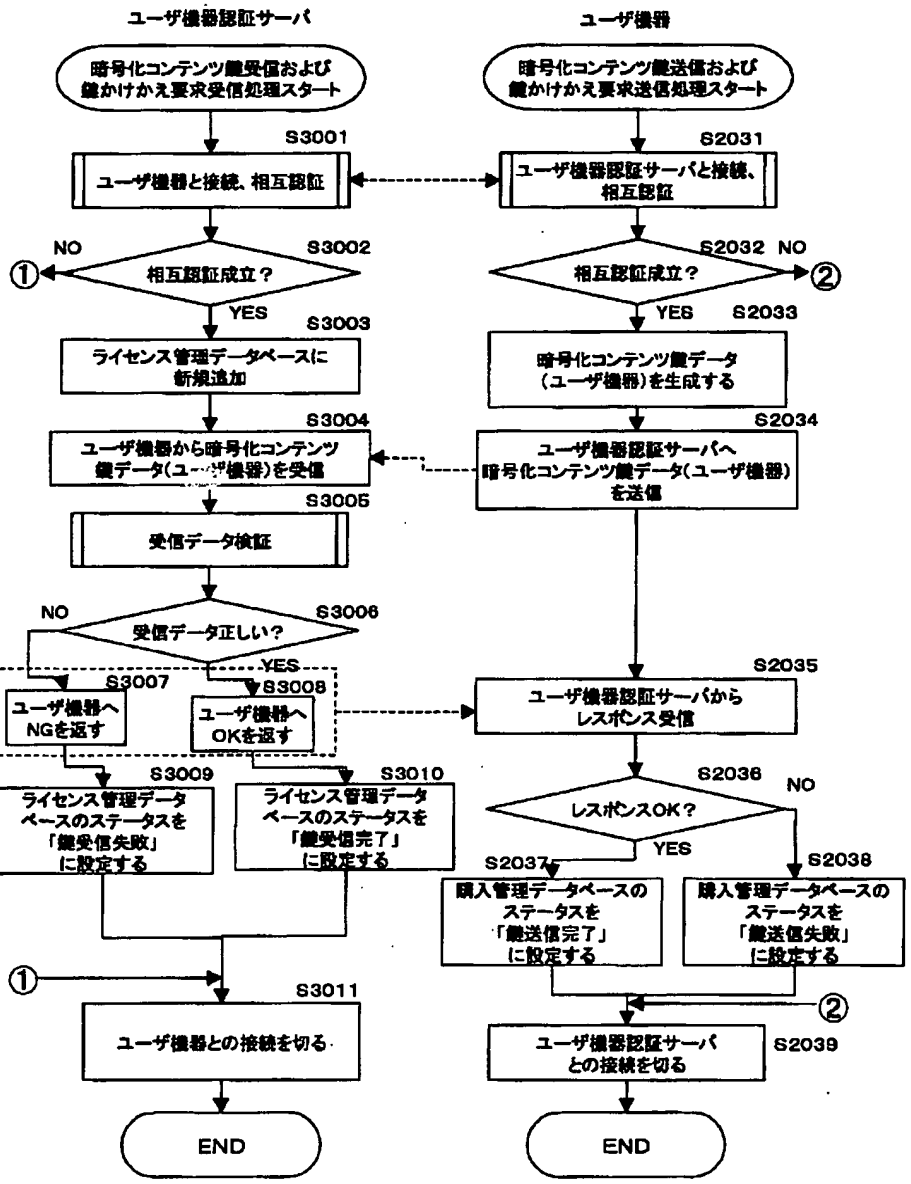
【図２４】


ショップサーバ
ユーザ機器
②
③
S2021
受信データの検証処理
S2022 NO
受信データは正しい？
YES
S1021
ユーザ機器からレスポンス
を受信する
S2023
ショップサーバへ
OKを返す
S2024
ショップサーバへ
NGを返す
S1022
NO
レスポンスはOKか？
YES
S2025
購入管理データベースの
ステータスを
「鍵1受信完了」にする
S2026
購入管理データベースの
ステータスを
「鍵1受信失敗」にする
S1023
購買管理データベースの
ステータスを
「鍵1配信失敗」にする
S1024
購買管理データベースの
ステータスを
「鍵1配信成功」にする
④
①
S1025
ユーザ機器との接続を切る
S2027
ショップサーバとの接続を切る
END
END

【図２３】


ショップサーバ
ユーザ機器
S1001
ユーザ機器と接続、相互認証
S2001
ショップサーバと接続、相互認証
NO
S1002
相互認証成立？
S2002
NO
YES
S1003
購買管理データベースに新規追加
YES
S2003
トランザクションIDを生成し、
購入管理データベースへ新規追加、
購入要求データを作成する。
S1004
ユーザ機器から購入要求データを受信
S2004
ショップサーバへ購入要求データを送信
S1005
受信データ検証
NO
S1008
受信データ正しい？
YES
S1007
ユーザ機器へ
NGを返す
S1008
ユーザ機器へ
OKを返す
S2005
ショップサーバからレスポンス受信
S1009
購買管理データベースの
ステータスを
「購入受付失敗」
に設定する
S1010
購買管理データベースの
ステータスを
「購入受付完了」
に設定する
S2006
NO
レスポンスOK？
YES
S2007
購入管理データベースの
ステータスを
「購入要求送信完了」
に設定する
S2008
購入管理データベースの
ステータスを
「購入要求送信失敗」
に設定する
S1011
暗号化コンテンツ鍵データ1(ショップ)
を生成する
S1012
ユーザ機器へ
暗号化コンテンツKc(コンテンツ)
を送信する
S2009
ショップサーバから
暗号化コンテンツKc(コンテンツ)
を受信する
S1013
ユーザ機器へ
暗号化コンテンツ鍵データ1(ショップ)
を送信する
S2010
ショップサーバから
暗号化コンテンツ鍵データ1(ショップ)
を受信する
①
②
③
④

【図２５】

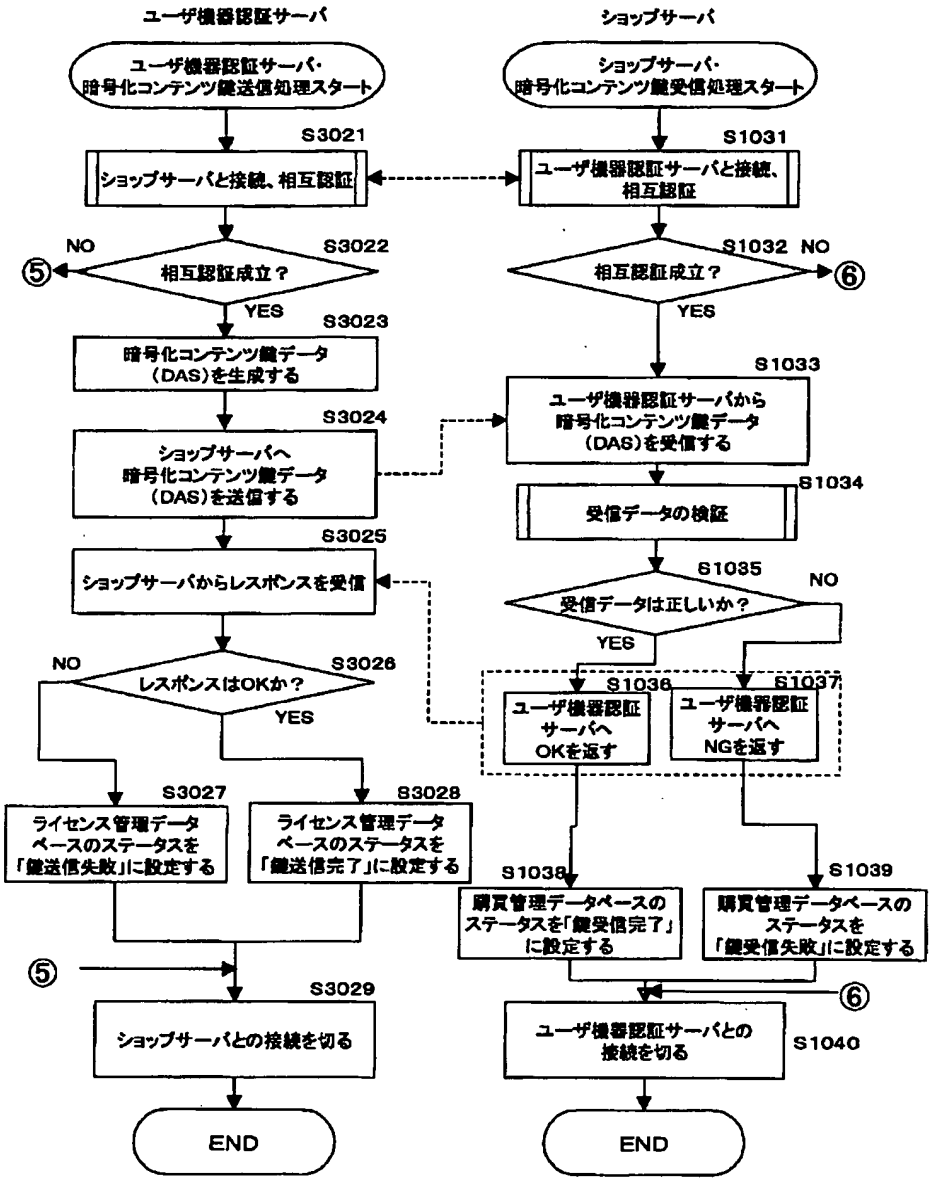


【図４５】

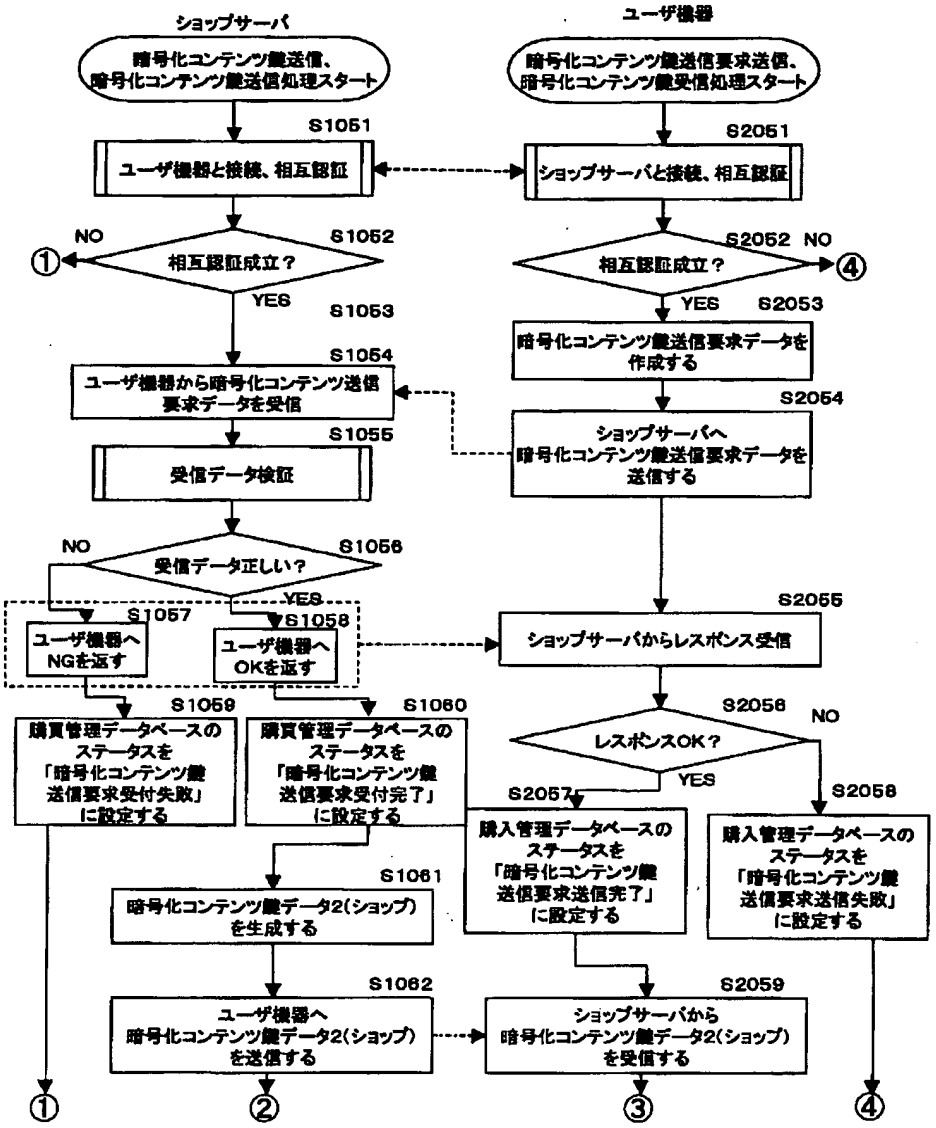
チケット換金サーバ処理No.	換金依頼元ID	チケット発行体ID	チケット発行処理No.	金額	機器ID	トランザクションID	ステータス
50001	12345	1234	10023	¥1000	1234567890	999888777	換金処理レポート送信完了
50002	23450	4455	10455	¥250	2345678901	666555444	換金処理完了
50003	33201	2354	10254	¥600	3456788901	321655444	電子チケット受信完了

チケット換金サーバ・チケット換金管理DB

【図２６】


ユーザ機器認証サーバ
ショップサーバ
ユーザ機器認証サーバ・暗号化コンテンツ鍵送信処理スタート
ショップサーバ・暗号化コンテンツ鍵受信処理スタート
S3021
ショップサーバと接続、相互認証
S1031
ユーザ機器認証サーバと接続、相互認証
NO
S3022
相互認証成立？
⑤
S1032
NO
相互認証成立？
⑥
YES
YES
S3023
暗号化コンテンツ鍵データ（DAS）を生成する
S1033
ユーザ機器認証サーバから暗号化コンテンツ鍵データ（DAS）を受信する
S3024
ショップサーバへ暗号化コンテンツ鍵データ（DAS）を送信する
S1034
受信データの検証
S3025
ショップサーバからレスポンスを受信
S1035
受信データは正しいか？
NO
YES
NO
S3026
レスポンスはOKか？
YES
S1036
ユーザ機器認証サーバへOKを返す
S1037
ユーザ機器認証サーバへNGを返す
S3027
ライセンス管理データベースのステータスを「鍵送信失敗」に設定する
S3028
ライセンス管理データベースのステータスを「鍵送信完了」に設定する
S1038
購買管理データベースのステータスを「鍵受信完了」に設定する
S1039
購買管理データベースのステータスを「鍵受信失敗」に設定する
⑤
⑥
S3029
ショップサーバとの接続を切る
ユーザ機器認証サーバとの接続を切る
S1040
END
END

【図２７】

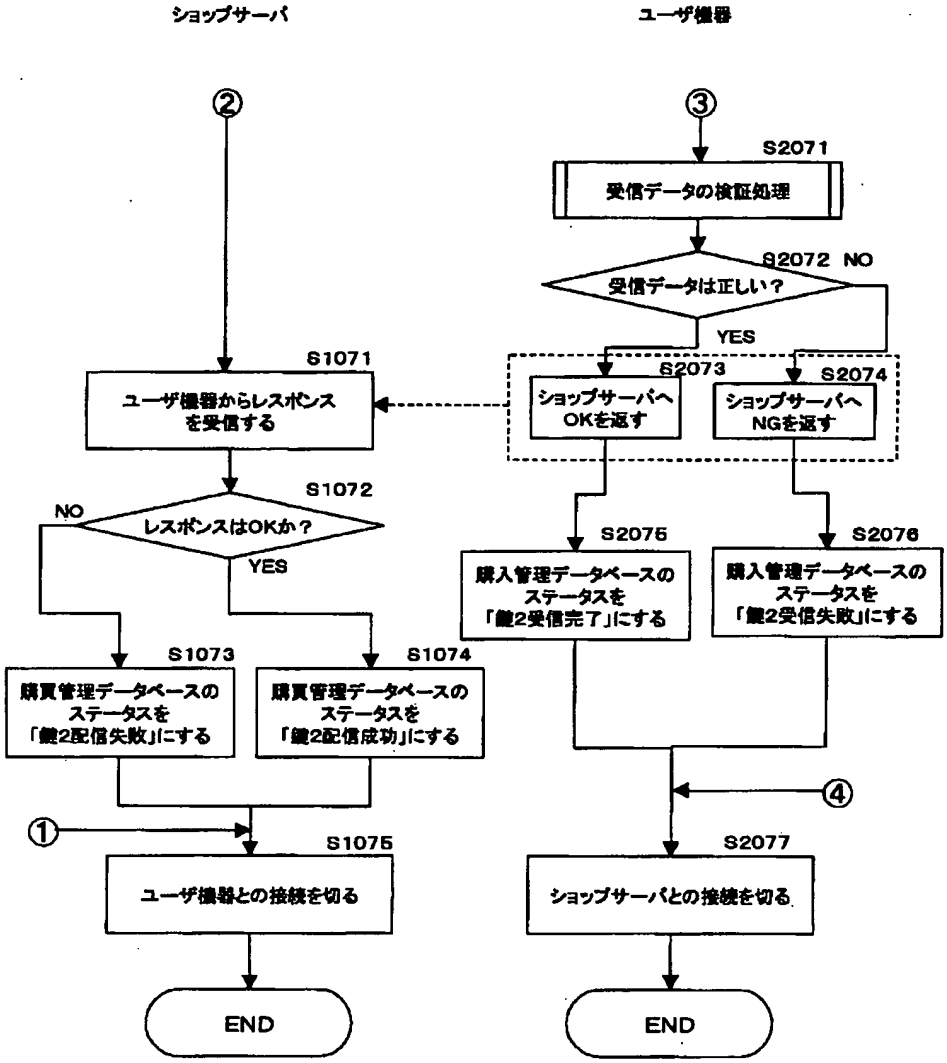


【図４３】

配信サーバ処理No.	コンテンツID	機器ID	チケット発行体ID	チケット発行処理No.	ステータス
999888777	5000	1234567890	1234	12345	換金処理レポート受信完了
666555444	4050	3427781534	2345	23456	チケット換金要求送信完了
999888779	5010	2355643551	1545	22335	配信完了
333555444	4320	4987390989	1030	32423	電子チケット受信完了
2133545445	3232	3542416759	2253	44323	電子チケット受信完了

配信サーバ・配信管理DB

【図２８】

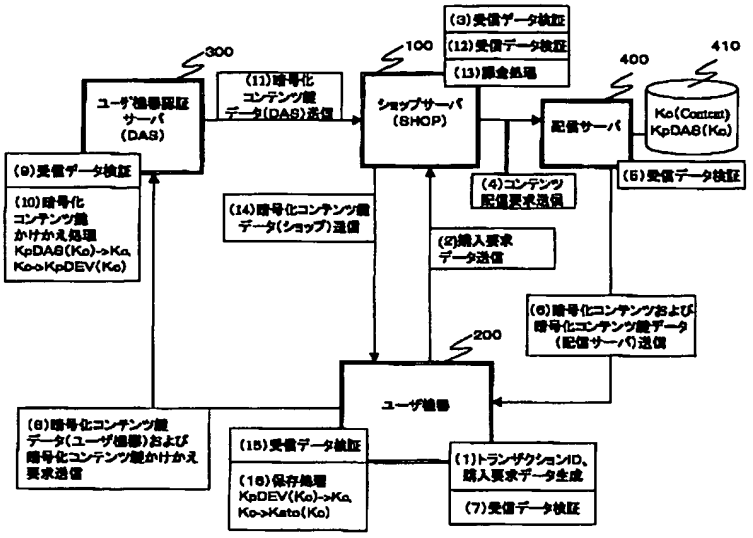


【図４０】

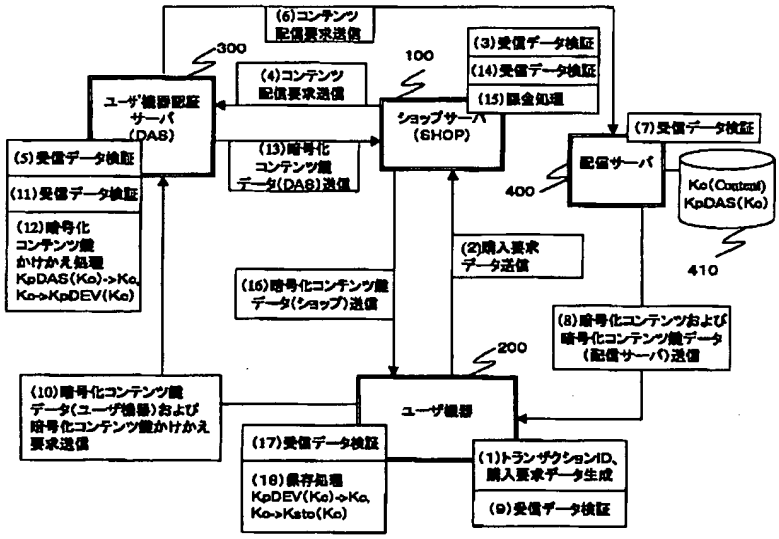
トランザクションID	コンテンツID	チケット発行体ID	チケット発行処理No.	チケット配信先ID	ステータス
999888777	5000	1234	10001	1234567890	鍵2受信完了
666555444	4050	1534	12345	2345678901	鍵1受信完了
999888779	5010	2351	15435	2233567890	電子チケット送信完了
333555444	4320	0989	10302	—	電子チケット受信完了
2133545445	3232	3549	22543	—	購入要求送信完了

ユーザ機器・購入管理DB

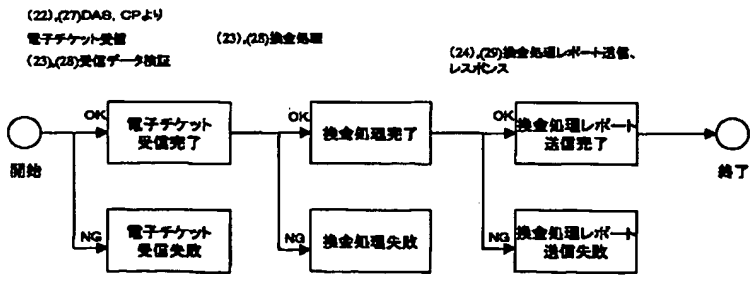
【図２９】


300
100
400
410
200
ユーザ機器認証サーバ (DAS)
ショップサーバ (SHOP)
配信サーバ
Ko(Content) KpDAS(Ko)
(3)受信データ検証
(12)受信データ検証
(13)課金処理
(11)暗号化コンテンツ鍵データ(DAS)送信
(5)受信データ検証
(4)コンテンツ配信要求送信
(9)受信データ検証
(10)暗号化コンテンツ鍵かけかえ処理 KpDAS(Ko)->Ko, Ko->KpDEV(Ko)
(14)暗号化コンテンツ鍵データ(ショップ)送信
(2)購入要求データ送信
(6)暗号化コンテンツおよび暗号化コンテンツ鍵データ(配信サーバ)送信
ユーザ機器
(8)暗号化コンテンツ鍵データ(ユーザ機器)および暗号化コンテンツ鍵かけかえ要求送信
(15)受信データ検証
(16)保存処理 KpDEV(Ko)->Ko, Ko->Kstb(Ko)
(1)トランザクションID、購入要求データ生成
(7)受信データ検証

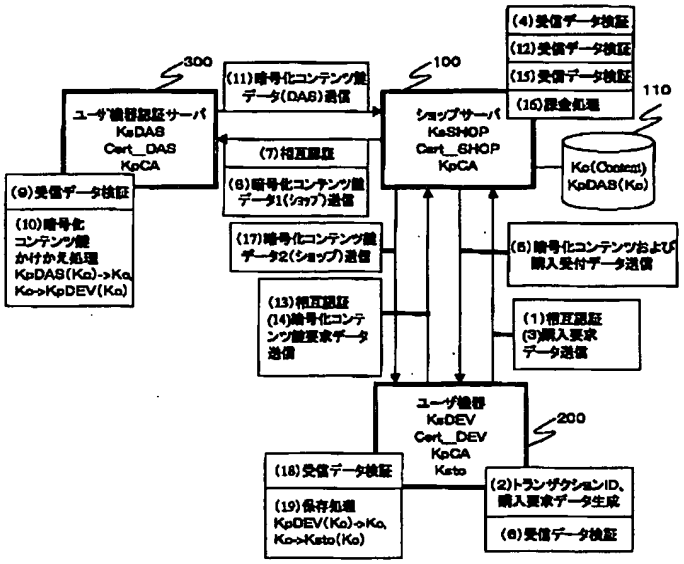
【図３０】


300
100
400
410
200
ユーザ機器認証サーバ (DAS)
ショップサーバ (SHOP)
配信サーバ
Ko(Content) KpDAS(Ko)
(6)コンテンツ配信要求送信
(4)コンテンツ配信要求送信
(3)受信データ検証
(14)受信データ検証
(15)課金処理
(7)受信データ検証
(5)受信データ検証
(11)受信データ検証
(13)暗号化コンテンツ鍵データ(DAS)送信
(12)暗号化コンテンツ鍵かけかえ処理 KpDAS(Ko)->Ko, Ko->KpDEV(Ko)
(2)購入要求データ送信
(16)暗号化コンテンツ鍵データ(ショップ)送信
(8)暗号化コンテンツおよび暗号化コンテンツ鍵データ(配信サーバ)送信
(10)暗号化コンテンツ鍵データ(ユーザ機器)および暗号化コンテンツ鍵かけかえ要求送信
ユーザ機器
(17)受信データ検証
(18)保存処理 KpDEV(Ko)->Ko, Ko->Kstb(Ko)
(1)トランザクションID、購入要求データ生成
(9)受信データ検証

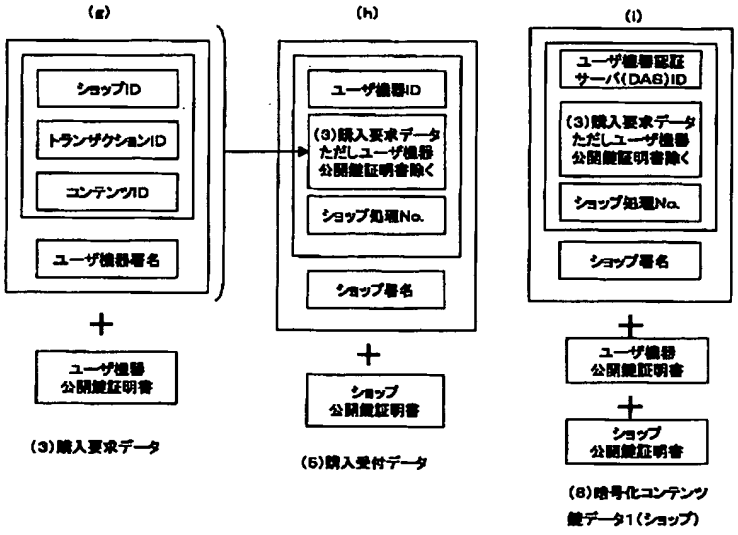
【図５２】


(22),(27)DAS、CPより電子チケット受信
(23),(25)課金処理
(24),(29)課金処理レポート送信、レスポンス
(23),(28)受信データ検証
開始
OK
電子チケット受信完了
課金処理完了
課金処理レポート送信完了
終了
NG
電子チケット受信失敗
課金処理失敗
課金処理レポート送信失敗

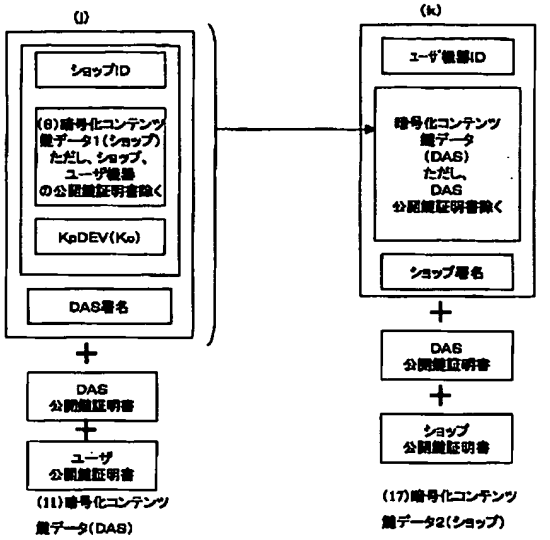
【図３１】


300
ユーザ機器認証サーバ
KsDAS
Cert_DAS
KpCA
(11)暗号化コンテンツ鍵データ(DAS)送信
(7)相互認証
(8)暗号化コンテンツ鍵データ1(ショップ)送信
(9)受信データ検証
(10)暗号化コンテンツ鍵かけかえ処理
KpDAS(Ko)->Ko
Ko->KpDEV(Ko)
100
ショップサーバ
KsSHOP
Cert_SHOP
KpCA
(4)受信データ検証
(12)受信データ検証
(15)受信データ検証
(16)課金処理
110
Ko(Content)
KpDAS(Ko)
(17)暗号化コンテンツ鍵データ2(ショップ)送信
(5)暗号化コンテンツおよび購入受付データ送信
(13)相互認証
(14)暗号化コンテンツ鍵要求データ送信
(1)相互認証
(3)購入要求データ送信
ユーザ機器
KsDEV
Cert_DEV
KpCA
Ksto
200
(18)受信データ検証
(19)保存処理
KpDEV(Ko)->Ko
Ko->Ksto(Ko)
(2)トランザクションID、購入要求データ生成
(6)受信データ検証

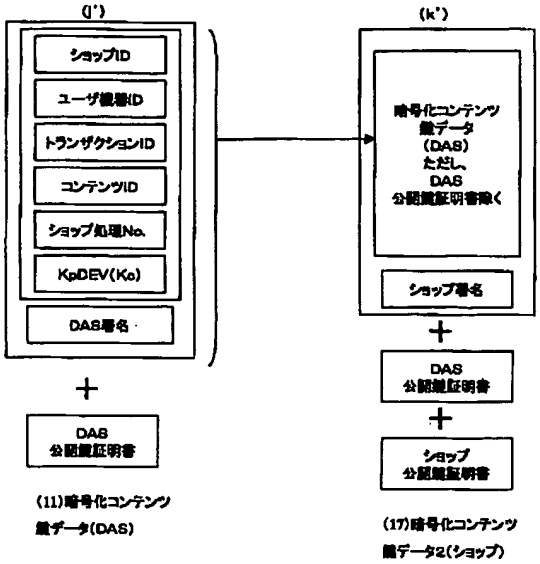
【図３２】


(g)
ショップID
トランザクションID
コンテンツID
ユーザ機器署名
+
ユーザ機器
公開鍵証明書
(3)購入要求データ
(h)
ユーザ機器ID
(3)購入要求データ
ただしユーザ機器
公開鍵証明書除く
ショップ処理No.
ショップ署名
+
ショップ
公開鍵証明書
(5)購入受付データ
(i)
ユーザ機器認証
サーバ(DAS)ID
(3)購入要求データ
ただしユーザ機器
公開鍵証明書除く
ショップ処理No.
ショップ署名
+
ユーザ機器
公開鍵証明書
+
ショップ
公開鍵証明書
(8)暗号化コンテンツ
鍵データ1(ショップ)

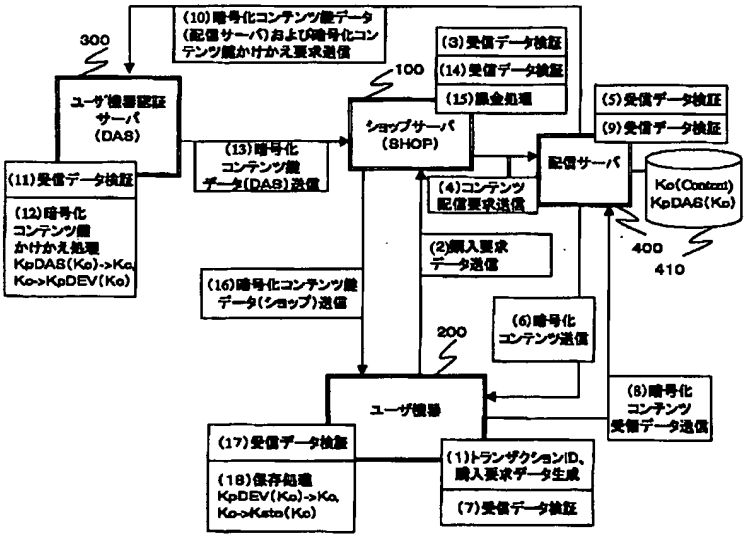
【図３３】



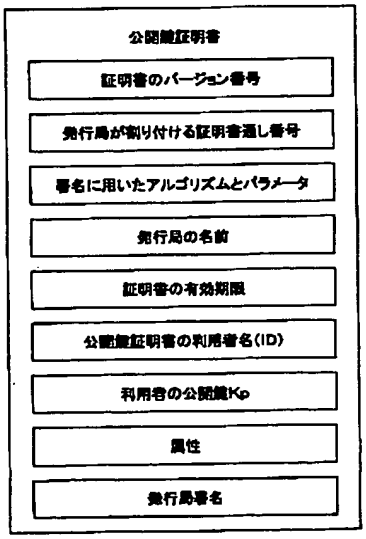
【図３４】



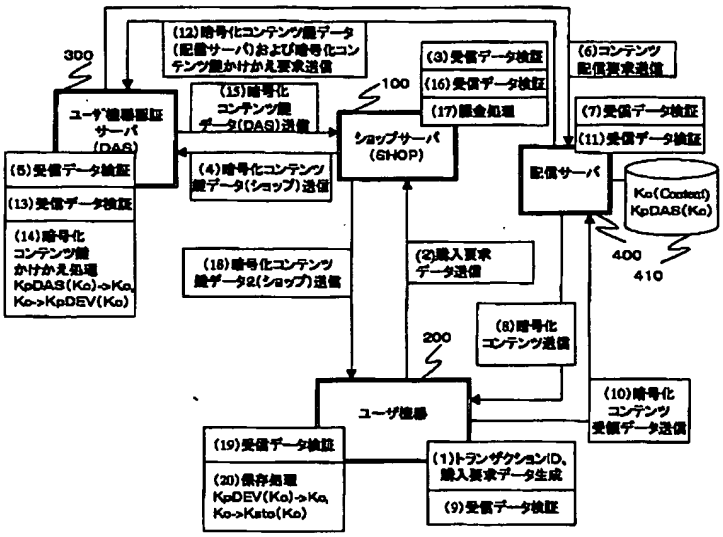
【図３５】



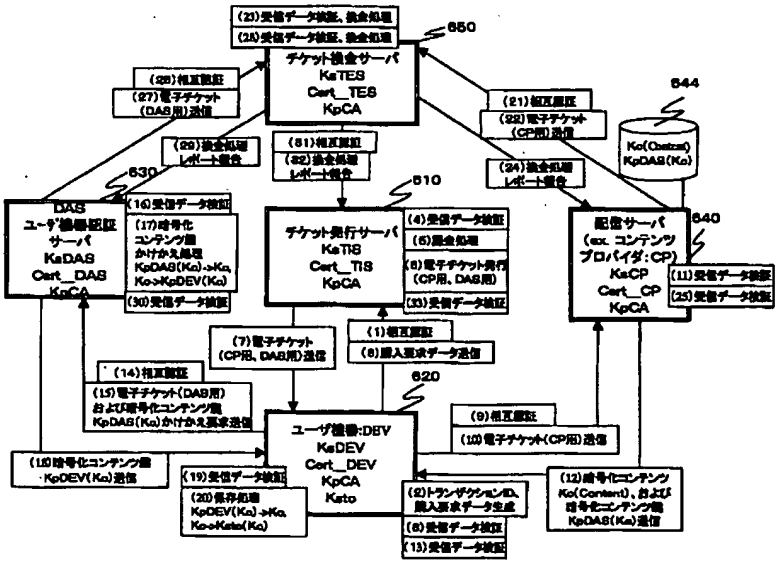
【図６７】



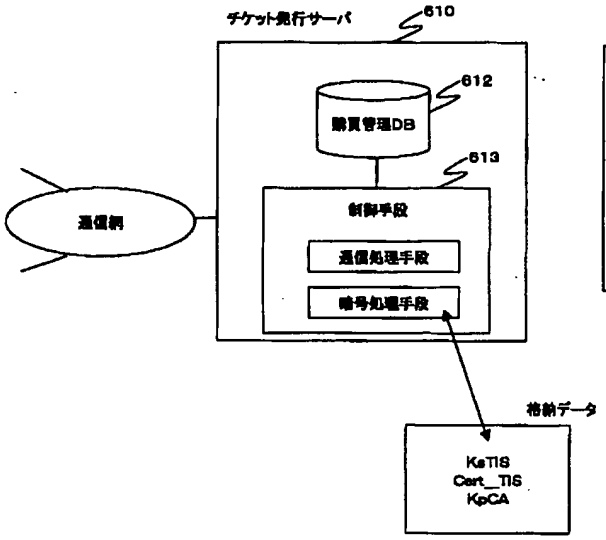
【図３６】


300
(12)暗号化コンテンツ鍵データ(配信サーバ)および暗号化コンテンツ鍵かけかえ要求送信
(3)受信データ検証
(16)受信データ検証
(17)課金処理
(6)コンテンツ配信要求送信
100
(15)暗号化コンテンツ鍵データ(DAS)送信
ユーザ機器認証サーバ(DAS)
ショップサーバ(SHOP)
(7)受信データ検証
(11)受信データ検証
配信サーバ
Ko(Content)
KpDAS(Ko)
(5)受信データ検証
(13)受信データ検証
(14)暗号化コンテンツ鍵かけかえ処理 KpDAS(Ko)->Ko, Ko->KpDEV(Ko)
(4)暗号化コンテンツ鍵データ(ショップ)送信
(18)暗号化コンテンツ鍵データ2(ショップ)送信
(2)購入要求データ送信
400
410
(8)暗号化コンテンツ送信
200
ユーザ機器
(10)暗号化コンテンツ受領データ送信
(19)受信データ検証
(20)保存処理 KpDEV(Ko)->Ko, Ko->Ksto(Ko)
(1)トランザクションID、購入要求データ生成
(9)受信データ検証

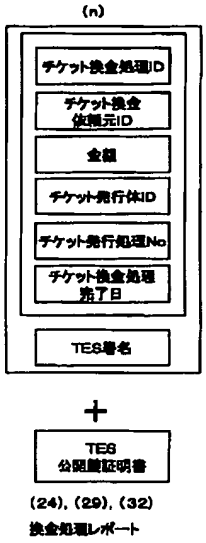
【図３７】


(23)受信データ検証、課金処理
(24)受信データ検証、課金処理
650
チケット課金サーバ KeTES Cert_TES KpCA
(28)相互認証
(27)電子チケット(DAS用)送信
(21)相互認証
(22)電子チケット(CP用)送信
644
Ko(Content) KpDAS(Ko)
(25)課金処理レポート報告
(31)相互認証
(32)課金処理レポート報告
(34)課金処理レポート報告
630
DAS ユーザ機器認証サーバ KeDAS Cert_DAS KpCA
(16)受信データ検証
(17)暗号化コンテンツ鍵かけかえ処理 KpDAS(Ko)->Ko, Ko->KpDEV(Ko)
(30)受信データ検証
610
チケット発行サーバ KeTIS Cert_TIS KpCA
(4)受信データ検証
(5)課金処理
(6)電子チケット発行(CP用、DAS用)
(33)受信データ検証
640
配信サーバ (ex. コンテンツプロバイダ:CP) KeCP Cert_CP KpCA
(11)受信データ検証
(25)受信データ検証
(7)電子チケット(CP用、DAS用)送信
(1)相互認証
(8)購入要求データ送信
(14)相互認証
(15)電子チケット(DAS用)および暗号化コンテンツ鍵 KpDAS(Ko)かけかえ要求送信
620
ユーザ機器:DEV KeDEV Cert_DEV KpCA Ksto
(9)相互認証
(10)電子チケット(CP用)送信
(18)暗号化コンテンツ鍵 KpDEV(Ko)送信
(19)受信データ検証
(20)保存処理 KpDEV(Ko)->Ko, Ko->Ksto(Ko)
(2)トランザクションID、購入要求データ生成
(9)受信データ検証
(13)受信データ検証
(12)暗号化コンテンツ Ko(Content)、および暗号化コンテンツ鍵 KpDAS(Ko)送信

【図３８】



【図４６】

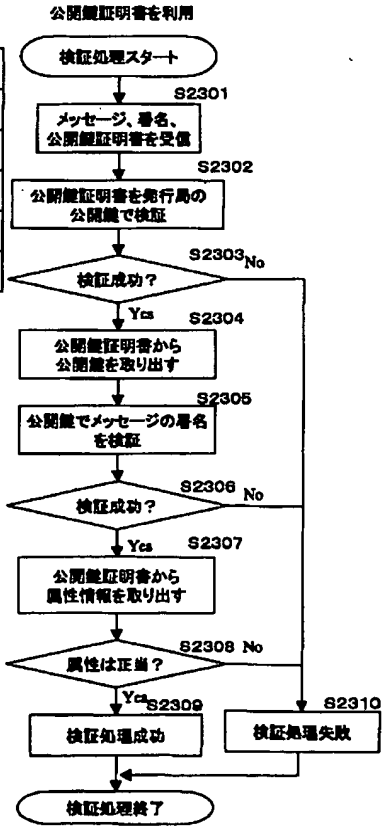


【図４１】

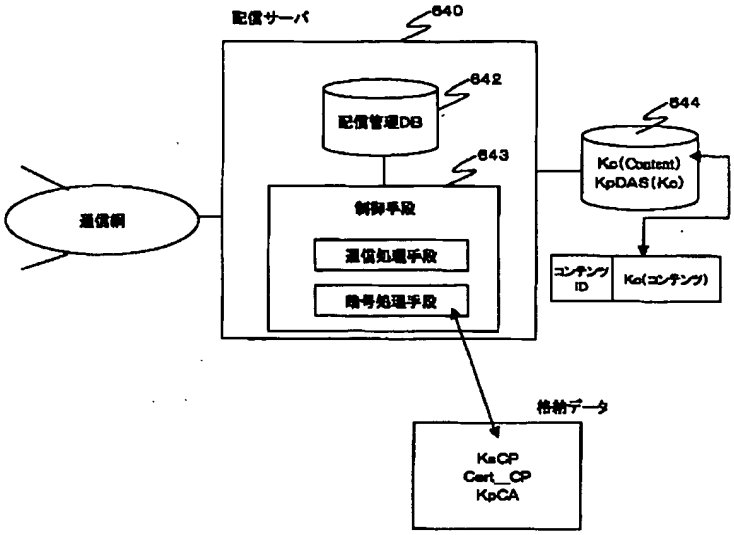
ユーザ機器認証サーバ処理No.	機器ID	トランザクションID	コンテンツID	チケット発行体ID	チケット発行処理No.	ステータス
50001	1234567890	999888777	5000	331234	10001	換金処理レポート受信完了
50002	2345678901	666555444	7050	345634	10025	チケット換金要求送信完了
50003	3456788901	321655444	8021	645234	10200	鍵送信完了
50004	5567778902	123555444	3245	321632	10325	鍵かけかえ完了
50005	5435678445	335655321	2651	764545	12300	鍵受信完了

ユーザ機器認証サーバ・ライセンス管理DB

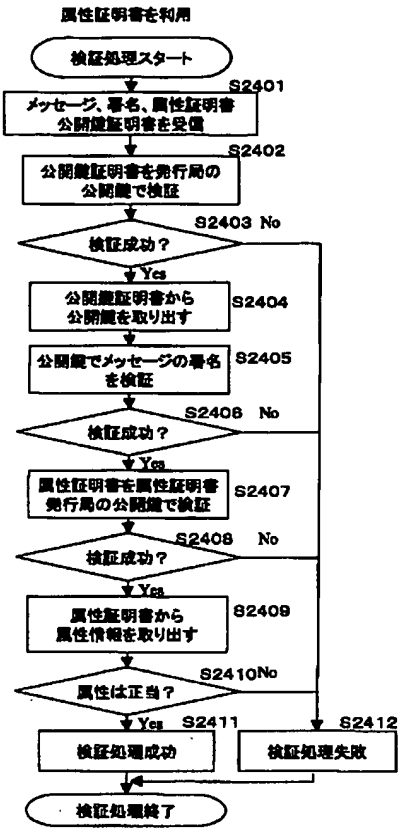
【図７５】



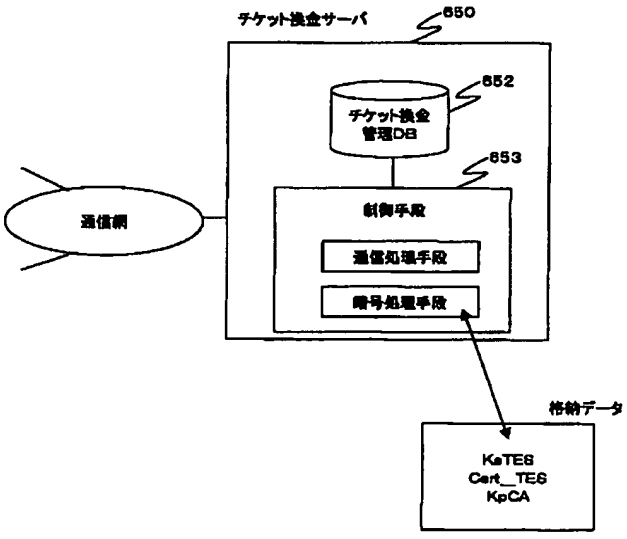
【図４２】


配信サーバ
640
642
配信管理DB
643
制御手段
通信処理手段
暗号処理手段
通信網
644
Ko(Content)
KpDAS(Ko)
コンテンツID
Ko(コンテンツ)
格納データ
KsCP
Cert_CP
KpCA

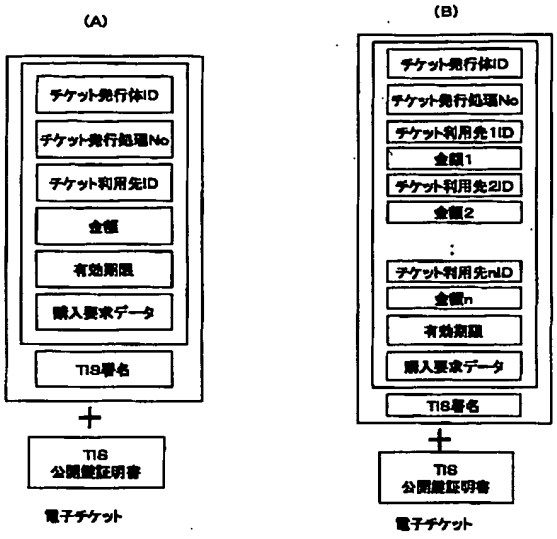
【図７６】


属性証明書を利用
検証処理スタート
S2401
メッセージ、署名、属性証明書
公開鍵証明書を受信
S2402
公開鍵証明書を発行局の
公開鍵で検証
S2403 No
検証成功？
Yes
公開鍵証明書から
公開鍵を取り出す
S2404
公開鍵でメッセージの署名
を検証
S2405
S2406 No
検証成功？
Yes
属性証明書を属性証明書
発行局の公開鍵で検証
S2407
S2408 No
検証成功？
Yes
属性証明書から
属性情報を取り出す
S2409
S2410No
属性は正当？
Yes
S2411
検証処理成功
S2412
検証処理失敗
検証処理終了

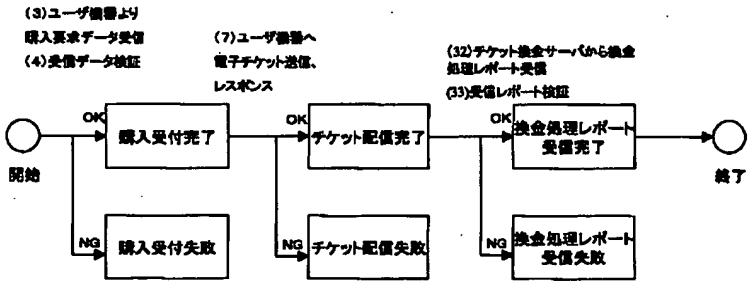
【図４４】


チケット換金サーバ
650
652
チケット換金
管理DB
653
制御手段
通信処理手段
暗号処理手段
通信網
格納データ
KsTES
Cert_TES
KpCA

【図４７】



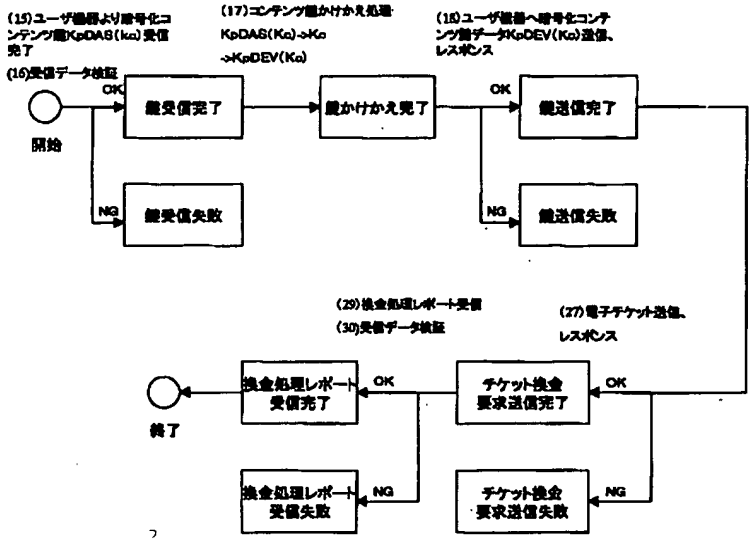
【図４８】



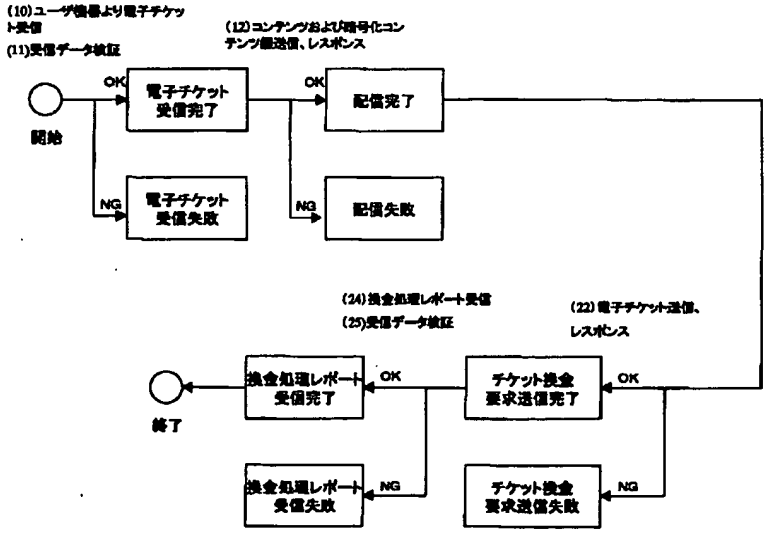
【図６６】

属性コード(2バイト)	エンティティ	機能
0000	登録局(RA)	公開鍵証明書、属性証明書の発行審査を行なう
0001	サービス運営者(SH)	システム上で流通するコンテンツのライセンス料を徴収する ex. コンテンツを復号するための鍵のかけ替え処理、ログ情報の収集
0002	コンテンツ販売者(SHOP)	ユーザにコンテンツ内容を提示し、コンテンツ販売代金を徴収する
0003	コンテンツ配信者	コンテンツ販売者の要求に応じ、ユーザにコンテンツを配信する
0004	ユーザ機器	コンテンツの購入、利用を行なう
:	:	:

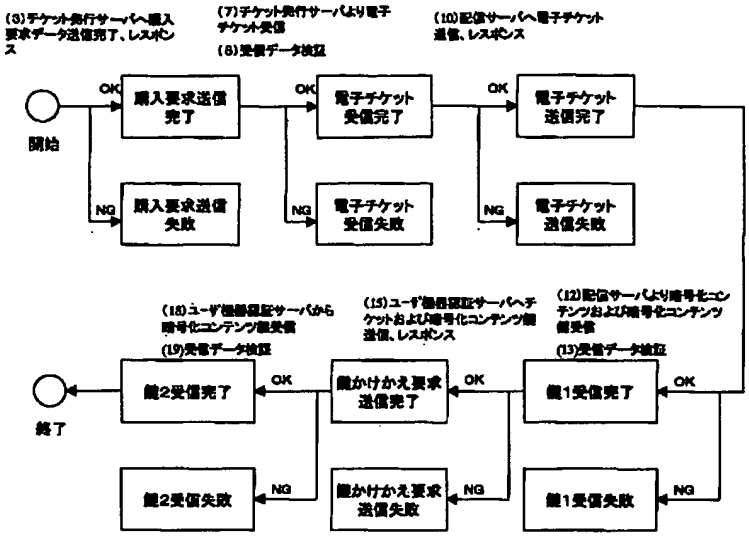
【図４９】


(15)ユーザ機器より暗号化コンテンツ鍵KpDAS(Kc)受信完了
(16)受信データ検証
(17)コンテンツ鍵かけかえ処理
KpDAS(Kc)->Kc
->KpDEV(Kc)
(18)ユーザ機器へ暗号化コンテンツ鍵データKpDEV(Kc)送信、レスポンス
OK
鍵受信完了
鍵かけかえ完了
OK
鍵送信完了
開始
NG
鍵受信失敗
NG
鍵送信失敗
(29)換金処理レポート受信
(30)受信データ検証
(27)電子チケット送信、レスポンス
換金処理レポート受信完了
OK
チケット換金要求送信完了
OK
終了
換金処理レポート受信失敗
NG
チケット換金要求送信失敗
NG

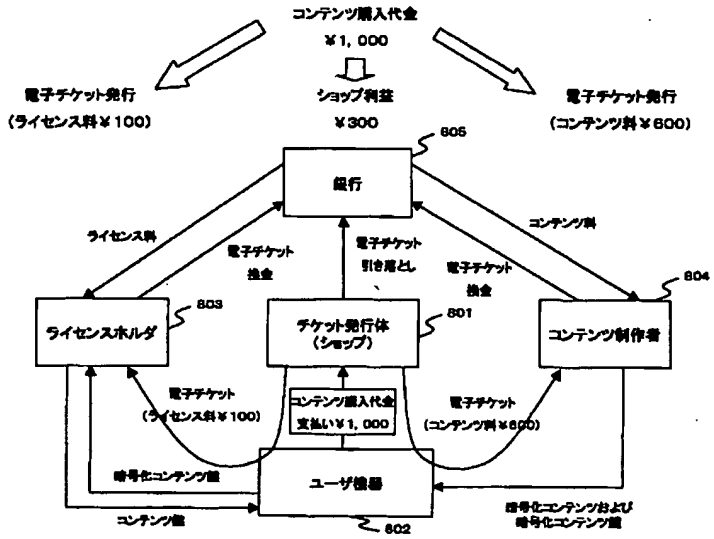
【図５０】


(10)ユーザ機器より電子チケット受信
(11)受信データ検証
(12)コンテンツおよび暗号化コンテンツ鍵送信、レスポンス
OK
電子チケット受信完了
OK
配信完了
開始
NG
電子チケット受信失敗
NG
配信失敗
(24)換金処理レポート受信
(25)受信データ検証
(22)電子チケット送信、レスポンス
換金処理レポート受信完了
OK
チケット換金要求送信完了
OK
終了
換金処理レポート受信失敗
NG
チケット換金要求送信失敗
NG

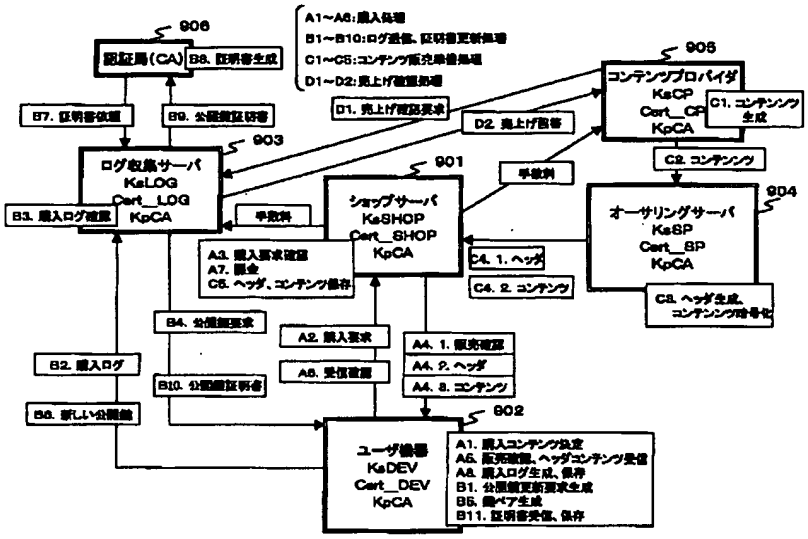
【図５１】


(8)チケット発行サーバへ購入要求データ送信完了、レスポンス
(7)チケット発行サーバより電子チケット受信
(6)受信データ検証
(10)配信サーバへ電子チケット送信、レスポンス
開始
OK
購入要求送信完了
電子チケット受信完了
電子チケット送信完了
NG
購入要求送信失敗
電子チケット受信失敗
電子チケット送信失敗
(18)ユーザ機器認証サーバから暗号化コンテンツ鍵受信
(19)受信データ検証
(15)ユーザ機器認証サーバへチケットおよび暗号化コンテンツ鍵送信、レスポンス
(12)配信サーバより暗号化コンテンツおよび暗号化コンテンツ鍵受信
(13)受信データ検証
終了
鍵2受信完了
鍵かけかえ要求送信完了
鍵1受信完了
鍵2受信失敗
鍵かけかえ要求送信失敗
鍵1受信失敗

【図５３】


コンテンツ購入代金
￥1，000
電子チケット発行
(ライセンス料￥100)
ショップ利益
￥300
電子チケット発行
(コンテンツ料￥600)
605
銀行
ライセンス料
電子チケット
振金
電子チケット
引き落とし
電子チケット
振金
コンテンツ料
804
803
801
ライセンスホルダ
チケット発行体
(ショップ)
コンテンツ制作者
電子チケット
(ライセンス料￥100)
コンテンツ購入代金
支払い￥1，000
電子チケット
(コンテンツ料￥600)
暗号化コンテンツ鍵
ユーザ機器
コンテンツ鍵
暗号化コンテンツおよび暗号化コンテンツ鍵
802

【図５４】



【図５５】

(A)

構成例1

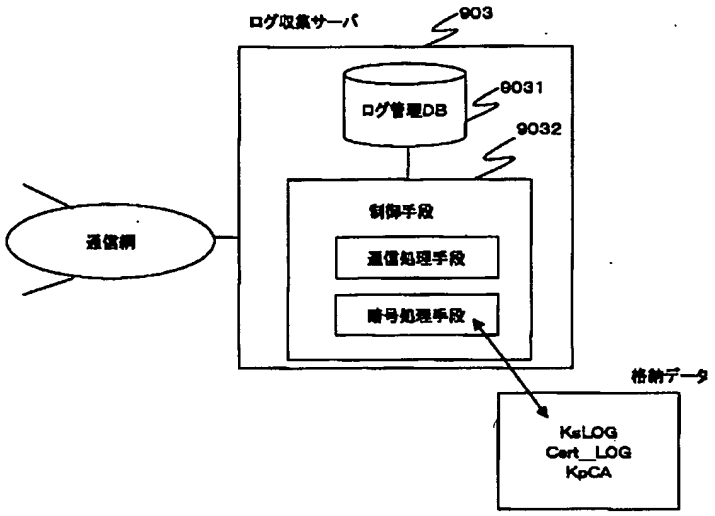
コンテンツID
ユーザ機器ID(ID_DEV)
ショップID(ID_SHOP)I
日付情報
ユーザ機器署名(Sig. Dev)

(B)

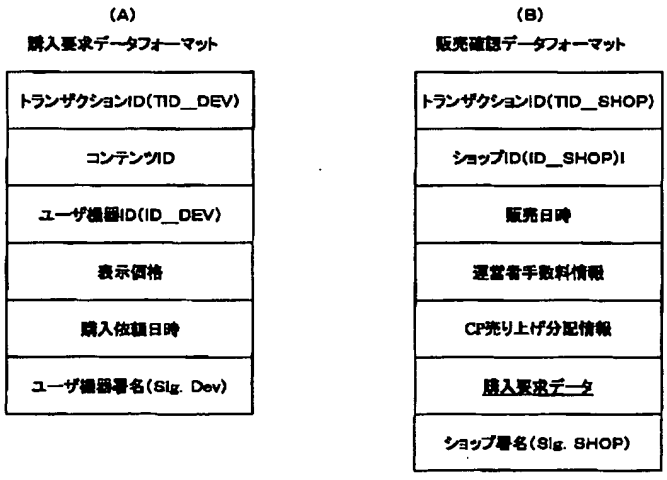
構成例2

販売確認データ
受け取り日時
ユーザ機器署名(Sig. Dev)

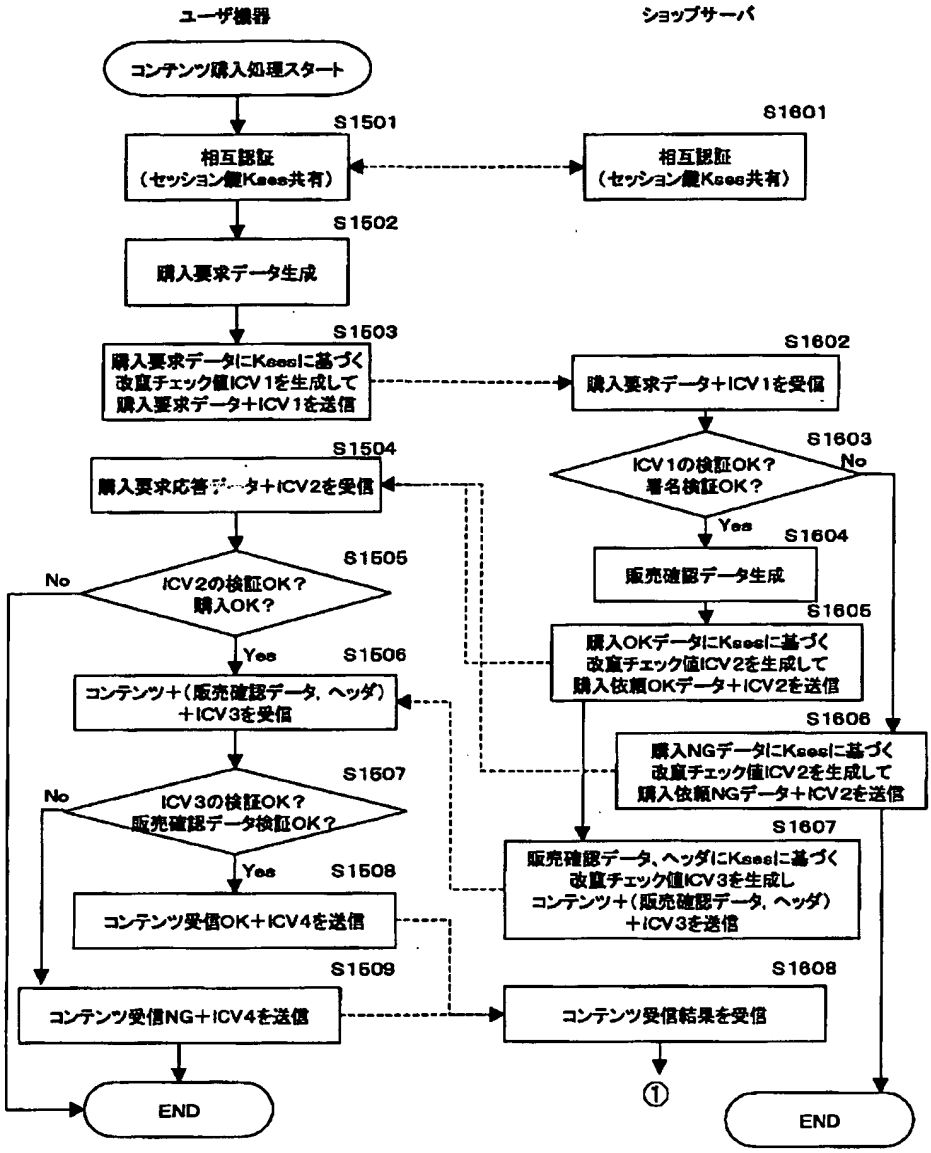
【図５６】


ログ収集サーバ
903
9031
ログ管理DB
9032
制御手段
通信処理手段
暗号処理手段
通信網
格納データ
KsLOG
Cert_LOG
KpCA

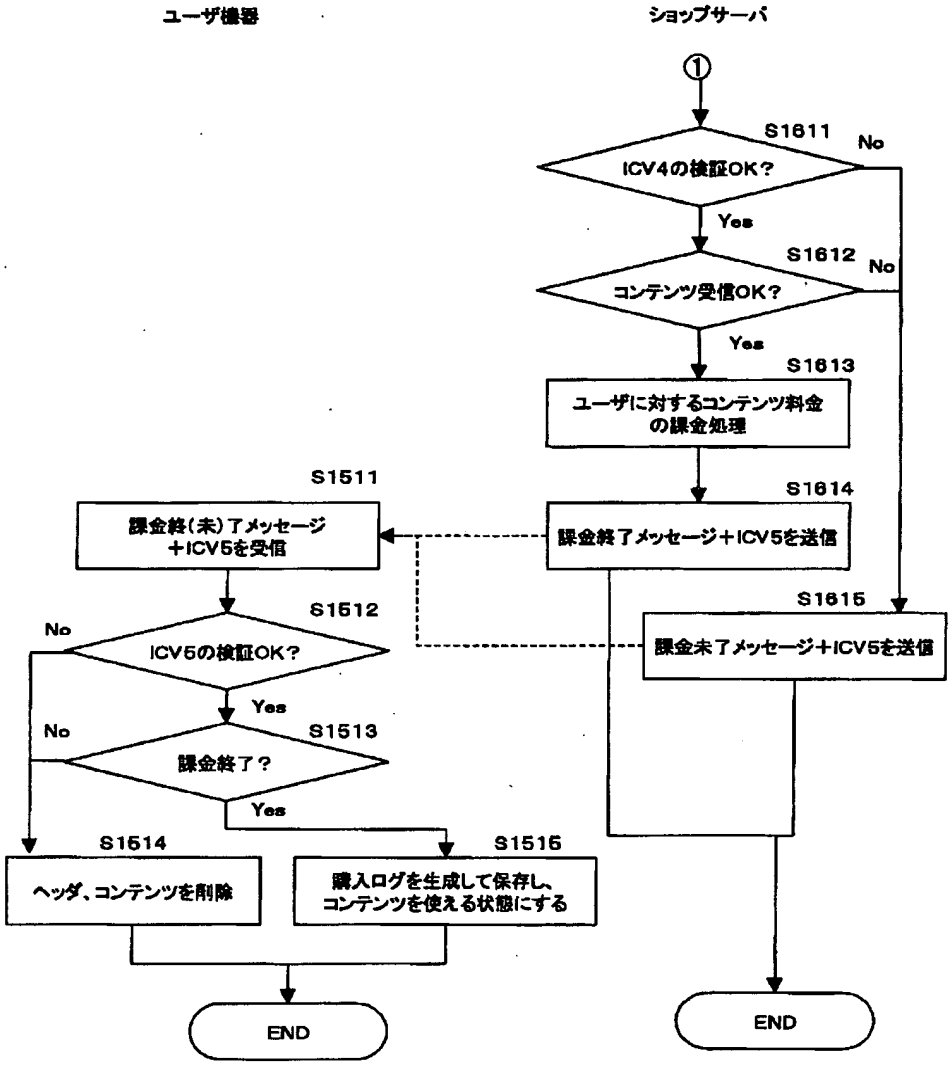
【図５９】


(A)
購入要求データフォーマット
トランザクションID(TID_DEV)
コンテンツID
ユーザ機器ID(ID_DEV)
表示価格
購入依頼日時
ユーザ機器署名(Sig. Dev)
(B)
販売確認データフォーマット
トランザクションID(TID_SHOP)
ショップID(ID_SHOP)I
販売日時
運営者手数料情報
CP売り上げ分配情報
購入要求データ
ショップ署名(Sig. SHOP)

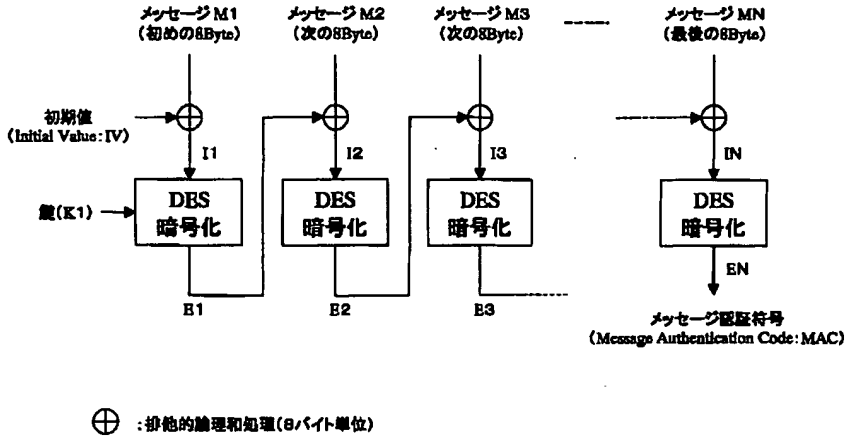
【図５７】


ユーザ機器
ショップサーバ
コンテンツ購入処理スタート
S1501
相互認証
（セッション鍵Kses共有）
S1601
相互認証
（セッション鍵Kses共有）
S1502
購入要求データ生成
S1503
購入要求データにKsesに基づく
改竄チェック値ICV1を生成して
購入要求データ+ICV1を送信
S1602
購入要求データ+ICV1を受信
S1603
ICV1の検証OK？
署名検証OK？
No
Yes
S1504
購入要求応答データ+ICV2を受信
S1604
販売確認データ生成
S1505
No
ICV2の検証OK？
購入OK？
S1605
購入OKデータにKsesに基づく
改竄チェック値ICV2を生成して
購入依頼OKデータ+ICV2を送信
Yes
S1506
コンテンツ+（販売確認データ，ヘッダ）
+ICV3を受信
S1606
購入NGデータにKsesに基づく
改竄チェック値ICV2を生成して
購入依頼NGデータ+ICV2を送信
S1607
No
ICV3の検証OK？
販売確認データ検証OK？
S1607
販売確認データ、ヘッダにKsesに基づく
改竄チェック値ICV3を生成し
コンテンツ+（販売確認データ，ヘッダ）
+ICV3を送信
Yes
S1508
コンテンツ受信OK+ICV4を送信
S1509
S1608
コンテンツ受信NG+ICV4を送信
コンテンツ受信結果を受信
①
END
END

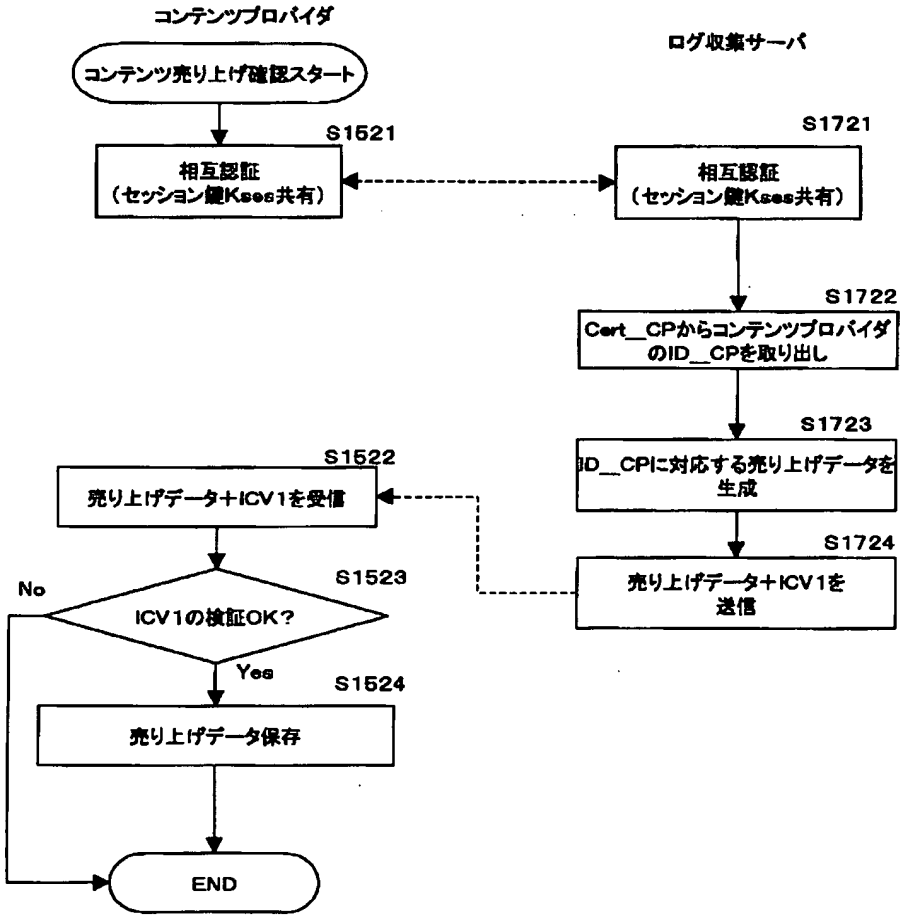
【図５８】


ユーザ機器
ショップサーバ
①
S1611
ICV4の検証OK?
No
Yes
S1612
コンテンツ受信OK?
No
Yes
S1613
ユーザに対するコンテンツ料金の課金処理
S1614
課金終了メッセージ+ICV5を送信
S1615
課金未了メッセージ+ICV5を送信
S1511
課金終(未)了メッセージ+ICV5を受信
S1512
ICV5の検証OK?
No
Yes
S1513
課金終了?
No
Yes
S1514
ヘッダ、コンテンツを削除
S1515
購入ログを生成して保存し、コンテンツを使える状態にする
END
END

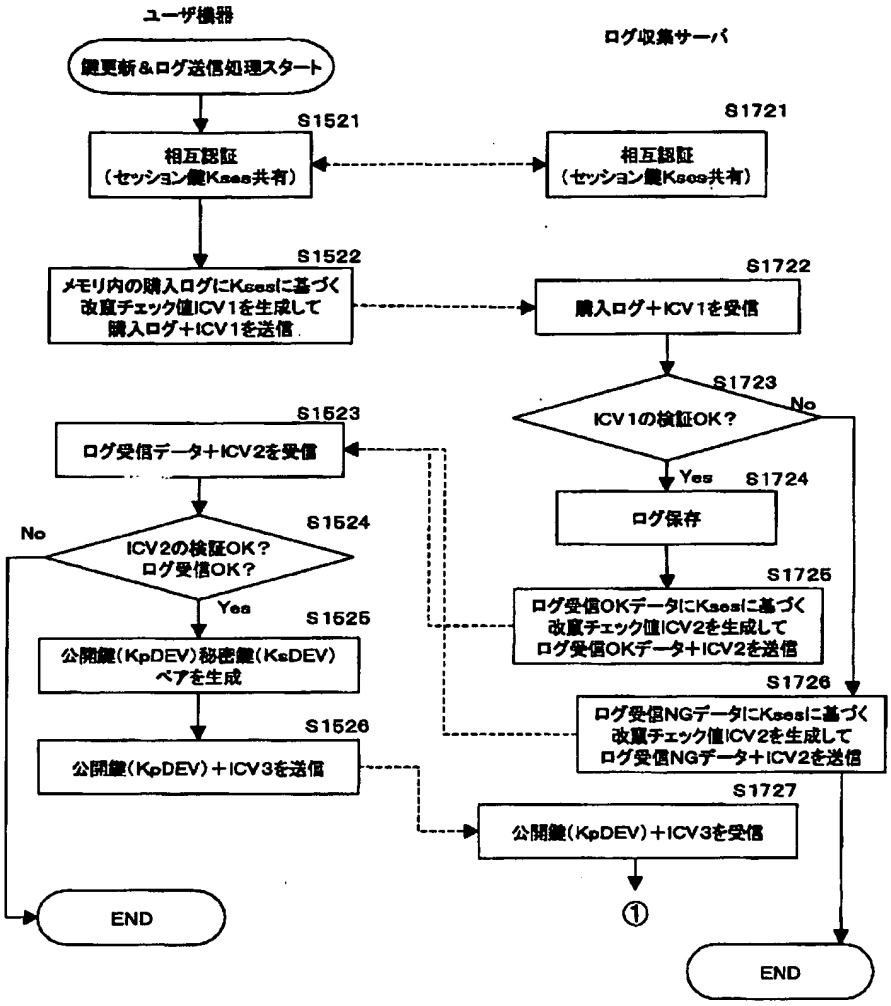
【図６０】


メッセージM1
(初めの8Byte)
メッセージM2
(次の8Byte)
メッセージM3
(次の8Byte)
メッセージMN
(最後の8Byte)
初期値
(Initial Value:IV)
I1
I2
I3
IN
鍵(K1)
DES
暗号化
DES
暗号化
DES
暗号化
DES
暗号化
E1
E2
E3
EN
メッセージ認証符号
(Message Authentication Code:MAC)
⊕ :排他的論理和処理(8バイト単位)

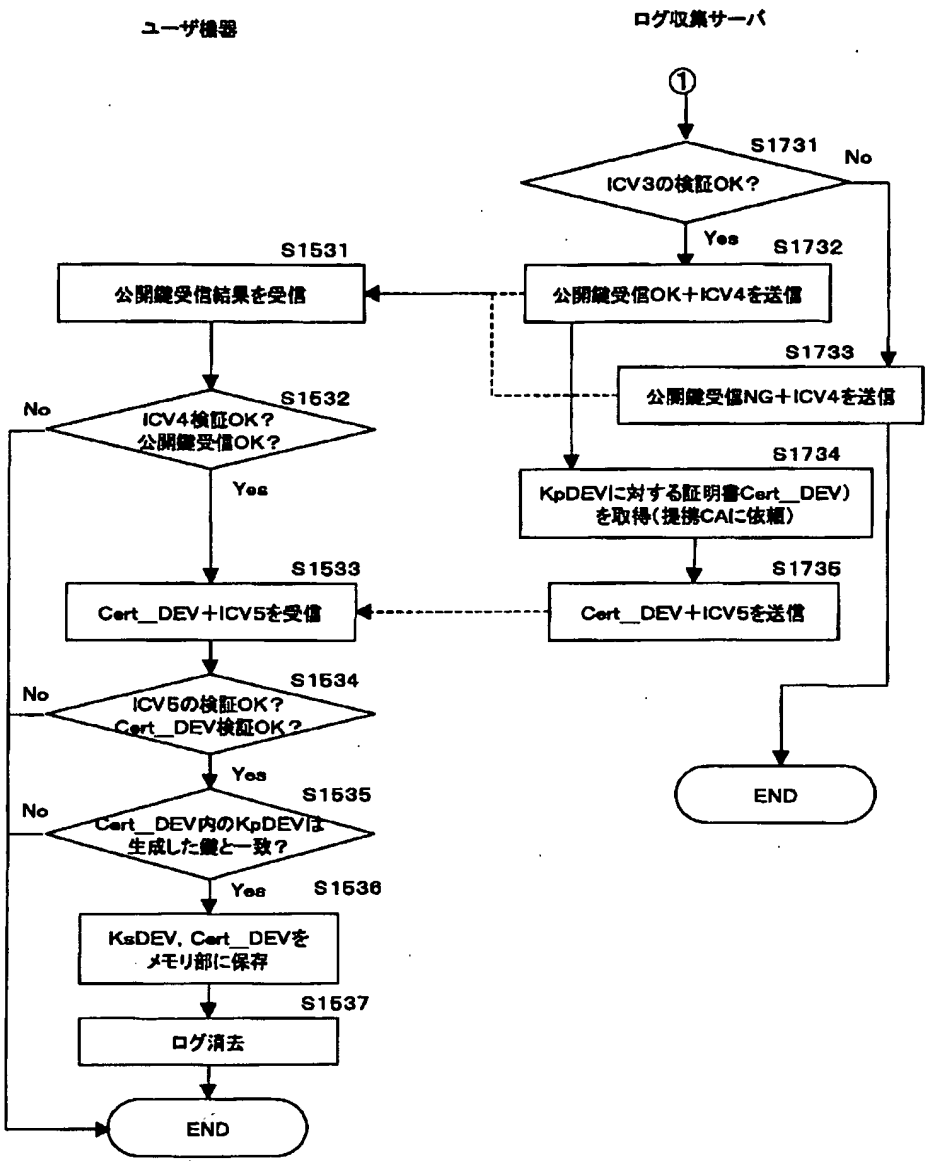
【図６３】


コンテンツプロバイダ
ログ収集サーバ
コンテンツ売り上げ確認スタート
S1521
相互認証
(セッション鍵Kses共有)
S1721
相互認証
(セッション鍵Kses共有)
S1722
Cert_CPからコンテンツプロバイダのID_CPを取り出し
S1723
ID_CPに対応する売り上げデータを生成
S1724
売り上げデータ+ICV1を送信
S1522
売り上げデータ+ICV1を受信
S1523
No
ICV1の検証OK?
Yes
S1524
売り上げデータ保存
END

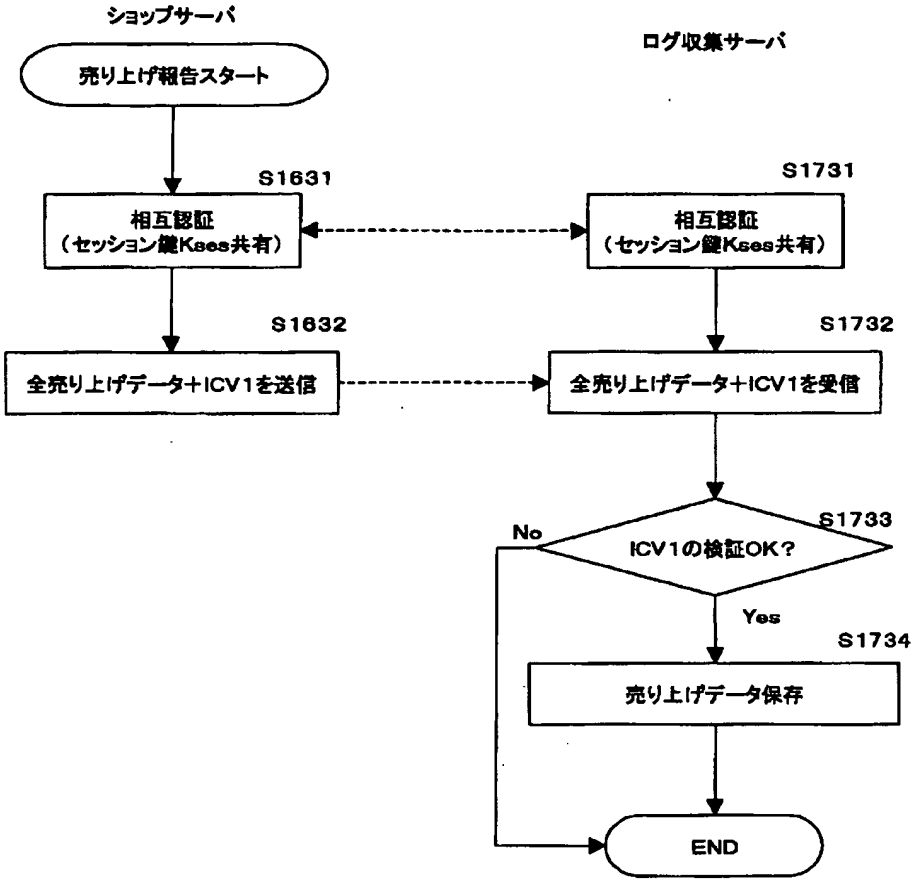
【図６１】


ユーザ機器
ログ収集サーバ
鍵更新&ログ送信処理スタート
S1521
相互認証
（セッション鍵Kses共有）
S1721
相互認証
（セッション鍵Kses共有）
S1522
メモリ内の購入ログにKsesに基づく
改竄チェック値ICV1を生成して
購入ログ＋ICV1を送信
S1722
購入ログ＋ICV1を受信
S1723
ICV1の検証OK？
No
Yes
S1724
ログ保存
S1523
ログ受信データ＋ICV2を受信
No
S1524
ICV2の検証OK？
ログ受信OK？
Yes
S1525
公開鍵(KpDEV)秘密鍵(KsDEV)
ペアを生成
S1725
ログ受信OKデータにKsesに基づく
改竄チェック値ICV2を生成して
ログ受信OKデータ＋ICV2を送信
S1726
ログ受信NGデータにKsesに基づく
改竄チェック値ICV2を生成して
ログ受信NGデータ＋ICV2を送信
S1526
公開鍵(KpDEV)＋ICV3を送信
S1727
公開鍵(KpDEV)＋ICV3を受信
①
END
END

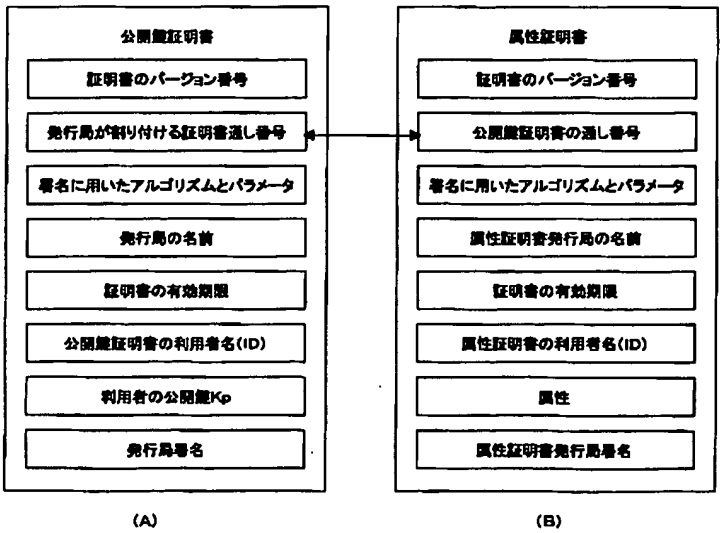
【図６２】


ユーザ機器
ログ収集サーバ
①
S1731
ICV3の検証OK？
No
Yes
S1732
公開鍵受信OK＋ICV4を送信
S1733
公開鍵受信NG＋ICV4を送信
S1734
KpDEVに対する証明書Cert_DEV）
を取得（提携CAに依頼）
S1735
Cert_DEV＋ICV5を送信
END
S1531
公開鍵受信結果を受信
S1532
No
ICV4検証OK？
公開鍵受信OK？
Yes
S1533
Cert_DEV＋ICV5を受信
S1534
No
ICV5の検証OK？
Cert_DEV検証OK？
Yes
S1535
No
Cert_DEV内のKpDEVは
生成した鍵と一致？
Yes
S1536
KsDEV, Cert_DEVを
メモリ部に保存
S1537
ログ消去
END

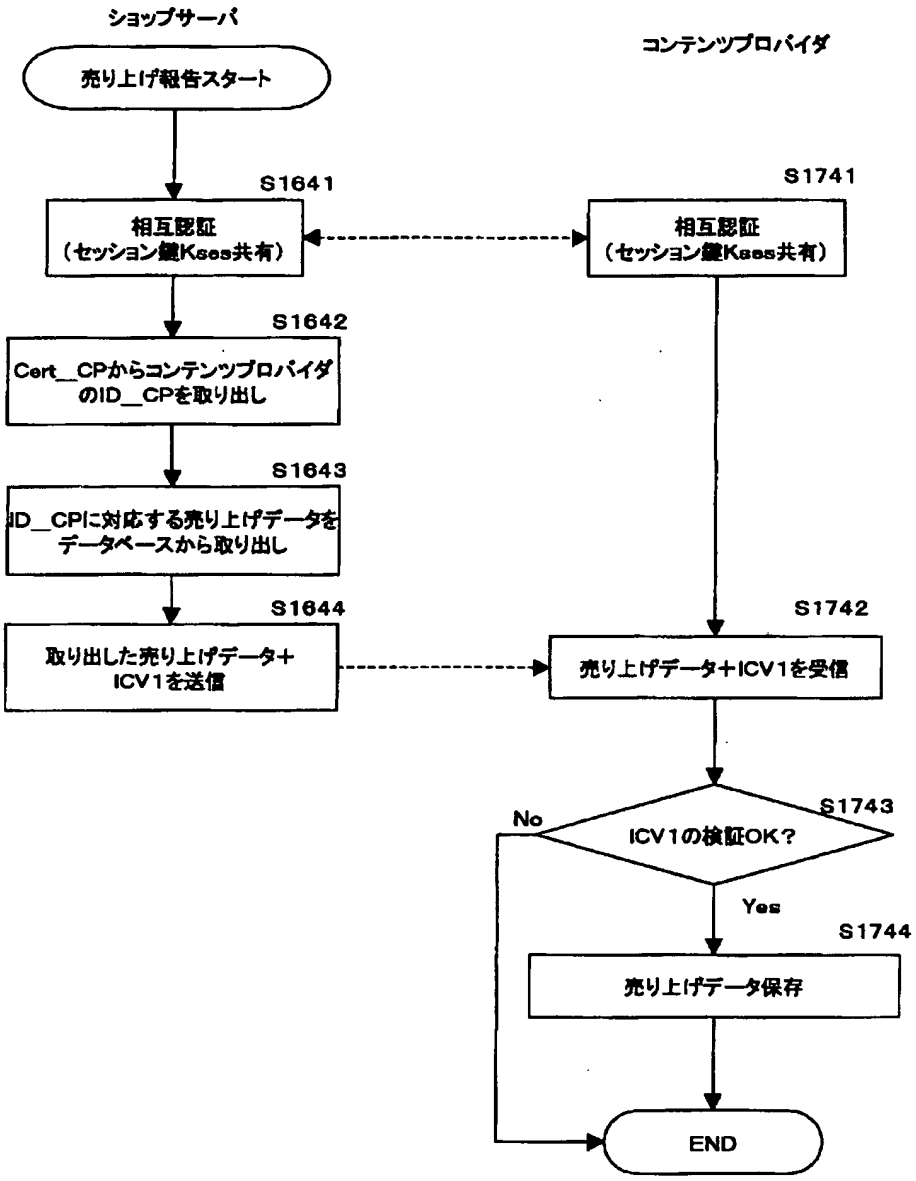
【図６４】


ショップサーバ
ログ収集サーバ
売り上げ報告スタート
S1631
相互認証
（セッション鍵Kses共有）
S1731
相互認証
（セッション鍵Kses共有）
S1632
全売り上げデータ+ICV1を送信
S1732
全売り上げデータ+ICV1を受信
No
S1733
ICV1の検証OK？
Yes
S1734
売り上げデータ保存
END

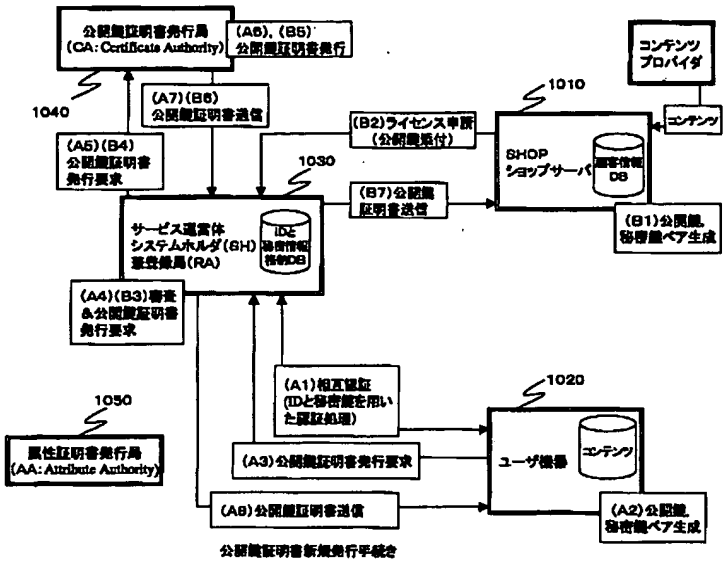
【図６８】


公開鍵証明書
証明書のバージョン番号
発行局が割り付ける証明書通し番号
署名に用いたアルゴリズムとパラメータ
発行局の名前
証明書の有効期限
公開鍵証明書の利用者名(ID)
利用者の公開鍵Kp
発行局署名
(A)
属性証明書
証明書のバージョン番号
公開鍵証明書の通し番号
署名に用いたアルゴリズムとパラメータ
属性証明書発行局の名前
証明書の有効期限
属性証明書の利用者名(ID)
属性
属性証明書発行局署名
(B)

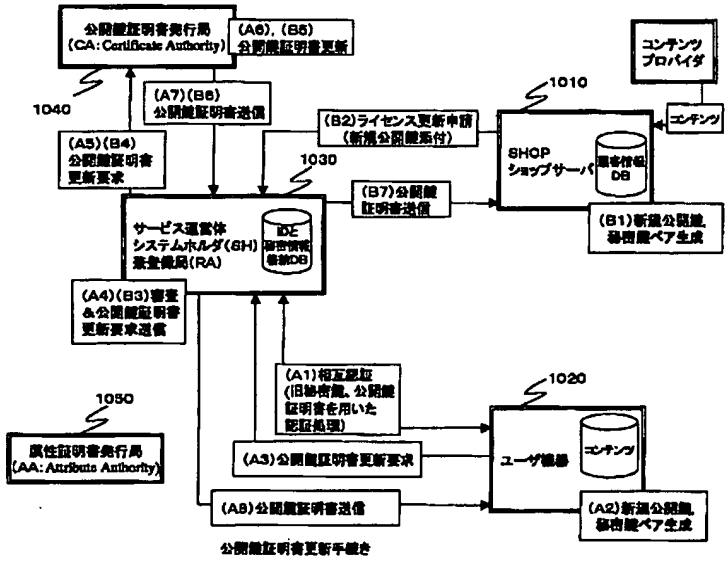
【図６５】


ショップサーバ
コンテンツプロバイダ
売り上げ報告スタート
S1641
相互認証
（セッション鍵Kses共有）
S1741
相互認証
（セッション鍵Kses共有）
S1642
Cert_CPからコンテンツプロバイダ
のID_CPを取り出し
S1643
ID_CPに対応する売り上げデータを
データベースから取り出し
S1644
取り出した売り上げデータ+
ICV1を送信
S1742
売り上げデータ+ICV1を受信
No
S1743
ICV1の検証OK?
Yes
S1744
売り上げデータ保存
END

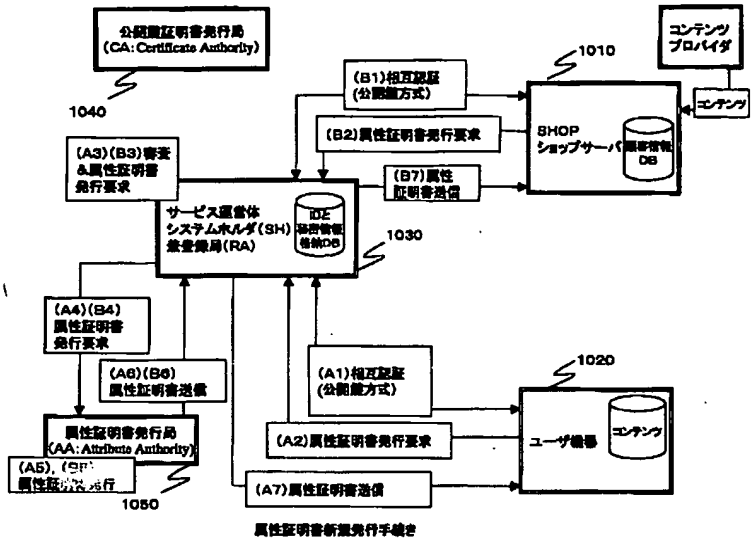
【図６９】


公開鍵証明書発行局
(CA: Certificate Authority)
(A5), (B5)
公開鍵証明書発行
1040
(A7)(B6)
公開鍵証明書送信
(A5)(B4)
公開鍵証明書
発行要求
1030
サービス運営体
システムホルダ(SH)
登録機関(RA)
IDと
秘密情報
登録DB
(A4)(B3)審査
&公開鍵証明書
発行要求
(B2)ライセンス申請
(公開鍵添付)
1010
SHOP
ショップサーバ
顧客情報
DB
コンテンツ
プロバイダ
コンテンツ
(B7)公開鍵
証明書送信
(B1)公開鍵,
秘密鍵ペア生成
1050
属性証明書発行局
(AA: Attribute Authority)
(A1)相互認証
(IDと秘密鍵を用い
た認証処理)
1020
(A3)公開鍵証明書発行要求
ユーザ機器
コンテンツ
(A8)公開鍵証明書送信
(A2)公開鍵,
秘密鍵ペア生成
公開鍵証明書新規発行手続き

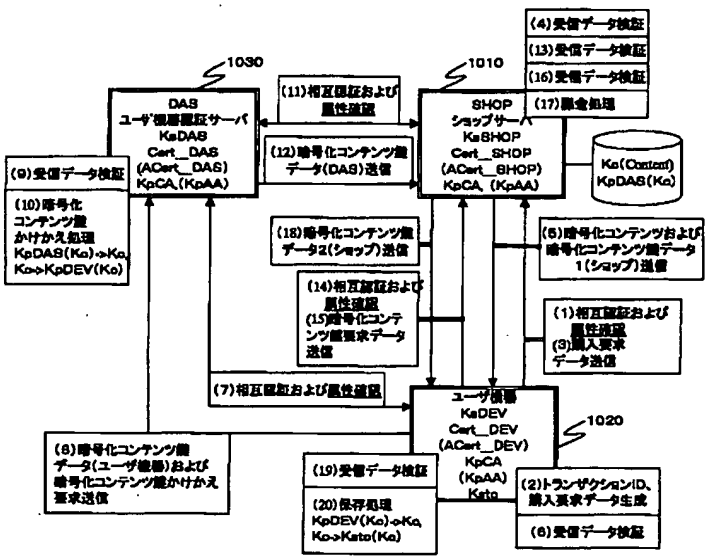
【図７０】


公開鍵証明書発行局
(CA: Certificate Authority)
(A6), (B5)
公開鍵証明書更新
1040
(A7)(B6)
公開鍵証明書送信
(A5)(B4)
公開鍵証明書
更新要求
1030
サービス運営体
システムホルダ(SH)
登録機関(RA)
IDと
秘密情報
登録DB
(A4)(B3)審査
&公開鍵証明書
更新要求送信
(B2)ライセンス更新申請
(新規公開鍵添付)
1010
SHOP
ショップサーバ
顧客情報
DB
コンテンツ
プロバイダ
コンテンツ
(B7)公開鍵
証明書送信
(B1)新規公開鍵,
秘密鍵ペア生成
1050
属性証明書発行局
(AA: Attribute Authority)
(A1)相互認証
(旧秘密鍵,公開鍵
証明書を用いた
認証処理)
1020
(A3)公開鍵証明書更新要求
ユーザ機器
コンテンツ
(A8)公開鍵証明書送信
(A2)新規公開鍵,
秘密鍵ペア生成
公開鍵証明書更新手続き

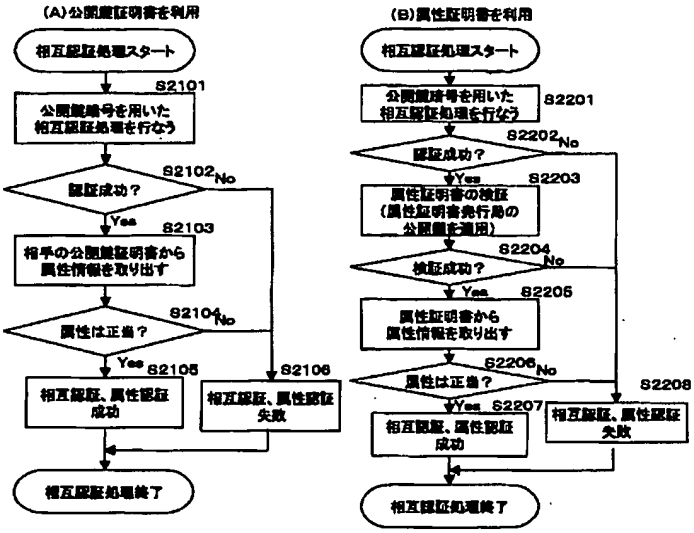
【図７１】


公開鍵証明書発行局
(CA:Certificate Authority)
1040
コンテンツ
プロバイダ
1010
(B1)相互認証
(公開鍵方式)
(B2)属性証明書発行要求
(B7)属性
証明書送信
SHOP
ショップサーバ
コンテンツ
(A3)(B3)審査
&属性証明書
発行要求
サービス運営体
システムホルダ(SH)
登録局(RA)
1030
(A4)(B4)
属性証明書
発行要求
(A6)(B6)
属性証明書送信
(A1)相互認証
(公開鍵方式)
1020
(A2)属性証明書発行要求
ユーザ端末
コンテンツ
属性証明書発行局
(AA:Attribute Authority)
(A5),(
属性証
1050
(A7)属性証明書送信
属性証明書新規発行手続き

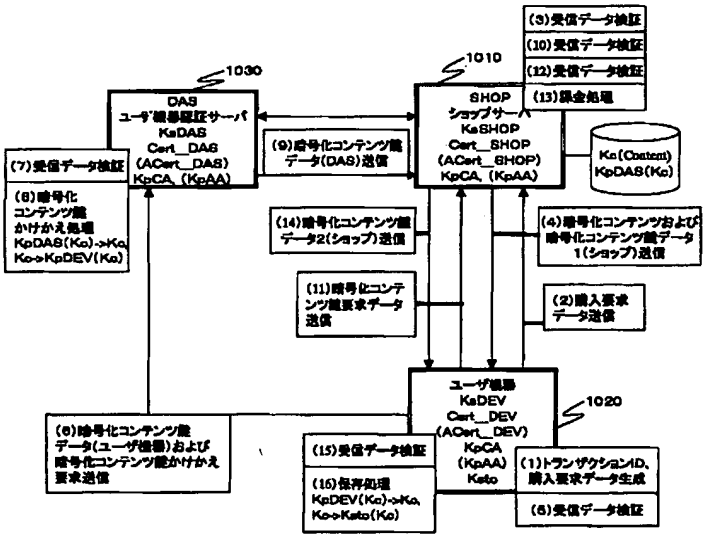
【図７２】


(4)受信データ検証
(13)受信データ検証
(16)受信データ検証
(17)課金処理
1030
DAS
ユーザ端末認証サーバ
KsDAS
Cert_DAS
(ACert_DAS)
KpCA_(KpAA)
(11)相互認証および
属性確認
1010
SHOP
ショップサーバ
KsSHOP
Cert_SHOP
(ACert_SHOP)
KpCA_(KpAA)
(12)暗号化コンテンツ鍵
データ(DAS)送信
Ks(Content)
KpDAS(Ks)
(9)受信データ検証
(10)暗号化
コンテンツ鍵
かけかえ処理
KpDAS(Ks)->Ks
Ks->KpDEV(Ks)
(18)暗号化コンテンツ鍵
データ2(ショップ)送信
(5)暗号化コンテンツおよび
暗号化コンテンツ鍵データ
1(ショップ)送信
(14)相互認証および
属性確認
(15)暗号化コンテン
ツ鍵要求データ
送信
(1)相互認証および
属性確認
(3)購入要求
データ送信
(7)相互認証および属性確認
ユーザ端末
KsDEV
Cert_DEV
(ACert_DEV)
KpCA
(KpAA)
Kstb
1020
(8)暗号化コンテンツ鍵
データ(ユーザ端末)および
暗号化コンテンツ鍵かけかえ
要求送信
(19)受信データ検証
(20)保存処理
KpDEV(Ks)->Ks
Ks->Kstb(Ks)
(2)トランザクションID、
購入要求データ生成
(6)受信データ検証

【図７３】



【図７４】



フロントページの続き

(51)Int.Cl.[7]		識別記号	FI		テーマコード（参考）
G06F	17/60	512	G09C	1/00	640B
G09C	1/00	640			640Z
			H04N	7/173	640Z
H04L	9/32		H04L	9/00	601B
H04N	7/167				675D
	7/173	640	H04N	7/167	Z

(72)発明者　石橋　義人
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　秋下　徹
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　白井　太三
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　岡　誠
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　吉森　正治
東京都港区赤坂七丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

Ｆターム(参考)　5B085 AE09 AE29
5C064 BA07 BB01 BB02 BB07 BC01
BC06 BC17 BC22 BD02 BD04
BD09 BD13 CA14 CB01 CC04
5J104 AA01 AA07 AA16 EA06 EA17
KA01 KA05 MA01 NA02 PA07